(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－250183
（P2003－250183A）
(43)公開日　平成15年９月５日(2003.9.5)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｑ　7/38		Ｇ０６Ｆ　12/14	３２０Ｆ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｋ　17/00	Ｓ	５Ｂ０３５
Ｇ０６Ｋ　17/00		Ｈ０４Ｍ　1/66		５Ｂ０５８
19/073		3/42	Ｚ	５Ｋ０２４
Ｈ０４Ｍ　1/66		Ｈ０４Ｂ　7/26	１０９Ｓ	５Ｋ０２７

審査請求　未請求　請求項の数25　ＯＬ　（全 31 頁）　最終頁に続く

(21)出願番号　特願2002－48904(P2002－48904)

(22)出願日　平成14年２月26日(2002.2.26)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　川野　眞二
東広島市鏡山３丁目10番18号株式会社松下電器情報システム広島研究所内

(72)発明者　辰巳　英典
東広島市鏡山３丁目10番18号株式会社松下電器情報システム広島研究所内

(74)代理人　100083172
弁理士　福井　豊明

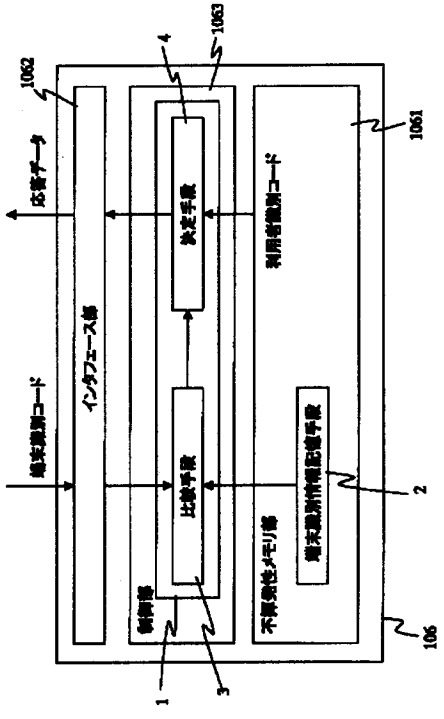
最終頁に続く

(54)【発明の名称】　ＩＣカード、端末、通信端末、通信局、通信機器及び通信制御方法

(57)【要約】

【課題】　携帯電話機などに取り外し可能に装着される利用者のＩＣカードが、紛失や盗難によって、悪意ある第三者の手に渡った場合でも、ＩＣカードに記憶されている利用者識別コードなどの情報が不正利用されたり漏洩したりするのを確実に回避する。

【解決手段】　ＩＣカードの端末識別情報記憶手段に携帯電話機を識別するための端末識別コードが記憶される。許可決定手段は、携帯電話機から入力された端末識別コードと端末識別情報記憶手段に記憶された端末識別コードとを比較する。許可決定手段は、その比較結果に基づいて、携帯電話機が要求する利用者識別コードなどを携帯電話機へ出力することを許可するか禁止するかを決定する。携帯電話機が悪意ある第三者のものである場合、端末識別コードは相違するから、利用者識別コードなどは出力されず、不正利用や漏洩が回避される。



【特許請求の範囲】

【請求項１】　端末に取り外し可能に装着され、該端末との間で情報の入出力を行うＩＣカードであって、
端末を識別するための端末識別情報を記憶する端末識別情報記憶手段と、
装着された端末から入力された端末識別情報と前記端末識別情報記憶手段に記憶された端末識別情報とを比較した比較結果に基づいて、端末が要求する要求情報を前記装着された端末へ出力することを許可するか禁止するかを決定する許可決定手段とを備えたＩＣカード。

【請求項２】　前記許可決定手段は、前記装着された端末の端末識別情報と前記端末識別情報記憶手段に記憶された端末識別情報が一致する場合に、前記要求情報の出力を許可し、前記端末識別情報が相違する場合に、前記要求情報の出力を禁止する請求項１記載のＩＣカード。

【請求項３】　前記端末識別情報とは別に前記要求情報の要求が正当であることを表す認証情報を記憶する認証情報記憶手段を備え、
前記許可決定手段は、前記端末識別情報が相違する場合に、前記装着された端末から入力された認証情報と前記認証情報記憶手段に記憶された認証情報とを比較し、前記認証情報も相違したときにのみ前記要求情報の出力を禁止する請求項２記載のＩＣカード。

【請求項４】　前記端末識別情報記憶手段には、前記許可決定手段によって前記要求情報の出力が前回許可された端末の端末識別情報が記憶される請求項３記載のＩＣカード。

【請求項５】　前記認証情報が一致したとき、前記端末識別情報記憶手段に記憶された端末識別情報を前記装着された端末の端末識別情報に更新する端末識別情報更新手段を備えた請求項４記載のＩＣカード。

【請求項６】　前記許可決定手段は、少なくとも前記要求情報が課金に利用される課金利用情報である場合、前記課金利用情報の出力を許可するか否かを決定する請求項３記載のＩＣカード。

【請求項７】　前記認証情報記憶手段は、前記認証情報だけでなく、電子商取引における認証に利用される取引用認証情報も記憶し、
前記許可決定手段は、前記端末識別情報が相違する場合に、前記認証情報が一致したとき、前記装着された端末から入力された取引用認証情報と前記認証情報記憶手段に記憶された取引用認証情報とを比較し、前記取引用認証情報も一致すれば前記課金利用情報の出力を許可する請求項６記載のＩＣカード。

【請求項８】　前記認証情報記憶手段の記憶内容を変更するための認証情報変更手段を備えた請求項３又は７記載のＩＣカード。

【請求項９】　前記課金利用情報は、利用者を識別するための利用者識別情報である請求項６記載のＩＣカード。

【請求項１０】　前記許可決定手段が前記装着された端末に前記要求情報を出力することを許可した場合に、前記装着された端末に出力される前記要求情報を暗号化する暗号化手段を備えた請求項１記載のＩＣカード。

【請求項１１】　前記端末識別情報記憶手段には、予め定められた１つ又は複数の端末に対する前記端末識別情報のみが記憶される請求項１記載のＩＣカード。

【請求項１２】　前記端末は移動通信端末である請求項１記載のＩＣカード。

【請求項１３】　請求項１記載のＩＣカードが取り外し可能に装着され、電気通信回線を通じて通信を行う通信端末であって、
自端末の端末識別情報を記憶する自端末識別情報記憶手段と、
前記自端末識別情報記憶手段に記憶された自端末の端末識別情報を装着されたＩＣカードに出力し、自端末の端末識別情報に対する前記装着されたＩＣカードの前記許可決定手段による決定に従い、前記要求情報を利用する通信を許可するか禁止するかを決定する通信許可決定手段とを備えた通信端末。

【請求項１４】　請求項３又は７記載のＩＣカードが取り外し可能に装着される端末であって、
前記認証情報記憶手段の記憶内容を変更するための認証情報変更手段を備えた端末。

【請求項１５】　通信機器と電気通信回線を介して通信に利用される通信端末と、前記通信端末に取り外し可能に装着され、前記通信端末との間で情報の入出力を行うＩＣカードとを備えた通信局であって、
前記ＩＣカードに備えられ、前記通信端末に出力される利用者を識別するための利用者識別情報を暗号化するための出力暗号化手段と、
前記通信端末に備えられ、前記通信端末に対する端末を識別するための端末識別情報を記憶する自端末識別情報記憶手段と、
前記自端末識別情報記憶手段に記憶された前記通信端末の端末識別情報と前記利用者識別情報との組合せを表す組合せ情報の少なくとも前記利用者識別情報が前記出力暗号化手段によって暗号化された暗号化組合せ情報を生成する暗号化組合せ情報生成手段と、
前記通信端末によって前記暗号化組合せ情報が送信された通信機器から、前記通信端末が、前記暗号化組合せ情報から復元された前記組合せ情報が正当な組合せを表すことを証明する証明情報を受信した場合にのみ、前記利用者識別情報を利用する通信を許可するか禁止するかを決定する通信許可決定手段とを備えた通信局。

【請求項１６】　前記暗号化組合せ情報生成手段は、前記通信端末に備えられ、前記自端末情報記憶手段に記憶された前記通信端末の端末識別情報と前記ＩＣカードから前記通信端末に出力された前記暗号化された利用者識別情報とを用いて前記暗号化組合せ情報を生成する請求

項１５記載の通信局。
【請求項１７】　前記暗号化組合せ情報生成手段は、前記ＩＣカードに備えられ、前記通信端末から前記ＩＣカードに入力された前記通信端末の端末識別情報と前記出力利用者識別情報暗号化手段によって暗号化された利用者識別情報とを用いて前記暗号化組合せ情報を生成する請求項１５記載の通信局。
【請求項１８】　前記出力暗号化手段は、利用者識別情報を記憶する利用者識別情報記憶手段と、前記利用者識別情報記憶手段に記憶された利用者識別情報を暗号化する利用者識別情報暗号化手段とを有する請求項１５記載の通信局。
【請求項１９】　前記出力暗号化手段は、前記通信機器が復号化に利用する秘密鍵に対応する公開鍵を用いて前記暗号化組合せ情報を生成する請求項１５記載のＩＣカード。
【請求項２０】　前記通信端末は移動通信端末である請求項１５記載のＩＣカード。
【請求項２１】　前記証明情報は、前記組合せ情報が正当なものであることが前記移動通信端末を移動体通信網に接続するための網接続装置によって証明されたものである請求項２０記載のＩＣカード。
【請求項２２】　前記証明情報は、前記組合せ情報が正当なものであることが電子商取引を管理する電子商取引サーバによって証明されたものである請求項１５記載のＩＣカード。
【請求項２３】　請求項１５記載の通信局と電気通信回線を介して通信を行う通信機器であって、
利用者識別情報と端末識別情報との組合せを記憶する組合せ記憶手段と、
前記通信局によって送信された前記暗号化組合せ情報から前記組合せ情報を復元する組合せ情報復元手段と、
前記組合せ記憶手段に記憶された利用者識別情報と端末識別情報との組合せのうち、前記組合せ情報復元手段によって復元された組合せ情報が表す利用者識別情報と端末識別情報との組合せと一致する組合せがある場合に、前記組合せ情報が正当な組合せを表すことを証明する証明情報を生成する証明情報生成手段とを備えた通信機器。
【請求項２４】　電気通信回線を介した通信に利用される通信端末と、前記通信端末に取り外し可能に装着され、前記通信端末との間で情報の入出力を行うＩＣカードとを備えた通信局が、前記通信端末を利用して行う通信を制御するための通信制御方法であって、
前記ＩＣカードに記憶されている端末を識別するための端末識別情報と前記通信端末から前記ＩＣカードに入力された前記通信端末の端末識別情報とを前記ＩＣカードが比較する手順と、
前記端末識別情報の比較結果に基づいて、前記通信端末が前記ＩＣカードに要求する要求情報を前記通信端末に出力することを許可するか禁止するかを前記ＩＣカードが決定する手順と、
前記ＩＣカードから前記通信端末に前記要求情報が出力された場合にのみ、前記通信端末が前記要求情報を利用する通信を行う手順とを備えた通信制御方法。
【請求項２５】　通信機器との電気通信回線を介した通信に利用される通信端末と、前記通信端末に取り外し可能に装着され、前記通信端末との間で情報の入出力を行うＩＣカードとを備えた通信局が、前記通信端末を利用して行う通信を制御するための通信制御方法であって、
前記ＩＣカードから前記通信端末に出力される利用者を識別するための利用者識別情報が暗号化された暗号化利用者情報と前記通信端末に記憶されている前記通信端末に対する端末を識別するための端末識別情報とを用いて、前記利用者識別情報と前記通信端末の端末識別情報との組合せを表す組合せ情報のうち少なくとも前記利用者識別情報が暗号化された暗号化組合せ情報を生成する手順と、
前記通信端末を用いて前記暗号化組合せ情報を通信機器に送信する手順と、
前記通信端末によって前記暗号化組合せ情報が送信された通信機器から、前記通信端末が、前記暗号化組合せ情報から復元された前記組合せ情報が正当な組合せを表すことを証明する証明情報を受信した場合にのみ、前記利用者識別情報を利用する通信を行う手順とを備えた通信制御方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、利用者を識別するための情報などが記憶されるＩＣカード、このＩＣカードが取り外し可能に装着される端末、通信端末、通信局、通信局が通信する通信機器及び通信制御方法に関するものである。
【０００２】
【従来の技術】第３世代の携帯電話機では、UIM (User Identity Module) と呼ばれるCPU(Central Processing Unit)を内蔵したIC(Integrated Circuit)カードが用いられる。UIMは、SIM (Subscriber Identity Module) と呼ばれるCPUを内蔵したICカードに対して上位互換性を有している。SIMは、世界的に普及しているGSM (Global System for Mobile Communications) 方式の携帯電話機(Mobile Subscriber)で用いられている。SIMやUIMは、通常携帯電話機の端末(Mobile Equipment)に取り外し可能に装着される。
【０００３】利用者の識別情報や電話番号などは、SIMやUIMに記憶される。これは、異なる端末で同じ電話番号を用いたり、異なる通信事業者のSIMやUIMを同じ端末で用いたりするためである。
【０００４】端末にSIMやUIMが装着されると、携帯電話機は、移動通信網における移動局(Mobile Station)とし

て動作する。例えば利用者がこれまで利用していた端末からSIMやUIMを取り外し、取り外したSIMやUIMを次に利用する端末に装着すれば、次の端末でこれまでの端末で使用していたのと同じ電話番号で通信することができる。

【０００５】また、端末にSIMやUIMが装着されなければ、携帯電話機は、緊急呼の場合を除いて通信できない。これは、SIMやUIMに識別情報が記憶された利用者を対象として通信料の課金が行われるためである。携帯電話機の端末からSIMやUIMを取り外すことによって端末と課金対象は独立するから、課金を行う通信事業者毎に端末に装着するSIMやUIMを変えれば、異なる通信事業者に対して同じ端末を利用することもできる。

【０００６】通信料の課金は、SIMやUIMに記憶された情報を基に行われるが、特にUIMは、通信サービスの他、電子商取引などでも広く利用されることが期待されており、この場合には、電子商取引における決済などもUIMに記憶された情報を基に行われることになる。取引明細や個人情報をUIMに記憶すれば、利用者の嗜好に応じたサービスを提供することもできる。

【０００７】携帯電話機は、UIMのようなICカードが提供する機能によって、通話や通信の手段としてだけでなく、商取引や身元証明など様々な用途においてインタフェースとして利用されることになる。

【０００８】このように携帯電話機の利用形態は多様化しつつあるが、携帯電話機やPDA(Personal Data Assistants)のような携帯端末で、利用者の識別情報や課金情報、個人情報などを管理する場合に問題となるのが、携帯端末の紛失や盗難である。

【０００９】携帯端末は、利用者が携帯することを前提として小型化されており、利用場所が限定されないことも多いから、紛失や盗難の危険性は少なくない。利用者の識別情報や課金情報、個人情報などが携帯端末で管理されている場合、紛失や盗難によって、携帯端末が悪意ある第三者の手に渡り、これらの情報が不正利用されたり、漏洩したりする恐れがある。携帯端末の利用形態が多様化すれば、不正利用などによって利用者が受ける被害も多様化し、被害がこれまでと較べて甚大になる可能性がある。

【００１０】このような被害を利用者が受けることを回避する技術として、特開２００１－１６８９８０号公報には、例えば移動通信端末が基地局から禁止信号を受信すると、移動通信端末が、クレジットカードのカード情報を記憶するメモリへのアクセスを禁止する技術が記載されている。

【００１１】紛失や盗難によって、携帯電話機が悪意ある第三者の手に渡った場合でも、ICカードが端末に装着されていれば、このような技術を用いてICカードへのアクセスを禁止することにより、ICカードに記憶された各種情報の不正使用を回避することができる。

【００１２】もっとも、ICカードが元の端末から取り外されるか、ICカードだけが紛失したり盗難にあったりした場合、ICカードが装着される端末は特定できないため、ICカードへのアクセスを禁止することができない。

【００１３】利用者が利用可能な端末が複数の場所にあれば、それらの場所の間では、ICカードだけを持ち運べばよいので、端末とICカードのうちICカードだけが紛失したり、盗難にあったりする恐れもある。携帯端末に取り外し可能に装着されるICカードは、プラグイン型のSIMやUIMのように、その大きさが切手ほどであることも多く、紛失の危険性は小さくない。

【００１４】このため、特開２０００－３０８１４０号公報に記載の技術では、移動無線通信装置本体が、端末本体に記憶している所有者を識別するための本体識別コードと、端末に装着されているICカードから読み出したICカードの所有者を識別するためのカード識別コードとに基づいて、通信を行うことを許可するか否かを決定している。

【００１５】この技術では、例えば前回の通信時に装着されていたのとは異なるICカードが移動無線通信装置本体に装着されていると、識別コードが一致せず、通信を行うことが禁止される。悪意ある第三者がICカードを入手した場合、移動無線通信装置本体には、それまでなかった新しいカードが装着されることになるから、通信の許可は行われず、そのICカードの不正利用が防止される。

【００１６】

【発明が解決しようとする課題】しかしながら、特開２０００－３０８１４０号公報に記載されているように、端末が識別コードの比較を行っていると、ICカードの装着された他の端末内の回路や信号を解析することによって、保護すべき情報が採取される恐れがある。

【００１７】また、端末に識別コードなどを記憶していると、悪意ある第三者の手に端末が渡った場合、端末の解析によってその情報が採取される恐れがある。さらに、異なる通信事業者のICカードが一つの端末に装着される場合、通信事業者毎に利用者の識別情報が異なれば、端末に各ICカードの識別コードを記憶することになるから、悪意ある第三者の手に端末が渡ると、これらの情報が一度に危険にさらされる。

【００１８】本発明は、このような従来の技術における課題を鑑みてなされたものであり、端末とその端末に取り外し可能に装着されるICカードのいずれかが悪意ある第三者の手に渡ったときでも、ICカードに記憶されている利用者の識別情報や課金情報、個人情報などの不正使用や漏洩を抑止することのできるICカード、端末、通信端末、通信局、通信局が通信する通信機器及び通信制御方法を提供することを目的とするものである。

【００１９】

【課題を解決するための手段】本発明は、上述の目的を

達成するために、以下の手段を採用している。

【００２０】例えば携帯電話機などの移動通信端末やその他の端末に取り外し可能に装着され、その端末との間で情報の入出力を行うＩＣカードにおいて、端末識別情報記憶手段に端末を識別するための端末識別情報が記憶される。許可決定手段は、装着された端末から入力された端末識別情報と端末識別情報記憶手段に記憶された端末識別情報とを比較する。そして、許可決定手段は、その比較結果に基づいて、端末が要求する要求情報を装着された端末へ出力することを許可するか禁止するかを決定する。

【００２１】例えば許可決定手段は、装着された端末の端末識別情報と端末識別情報記憶手段に記憶された端末識別情報が一致する場合に、要求情報の出力を許可し、端末識別情報が相違する場合に、要求情報の出力を禁止する。

【００２２】悪意ある第三者がＩＣカードだけを入手しても、その場合、端末とＩＣカードの組合せが相違する。比較結果によって要求情報の出力を許可するか禁止するかが決定されるから、悪意ある第三者がＩＣカードに記憶された情報を他の端末を用いて不正使用することはできない。また、ＩＣカードが装着された他の端末を解析しても、要求情報がその端末に出力されないから、端末からそれらを採取することもできない。さらに、端末にＩＣカードに関する情報を記憶する必要がないので、ＩＣカードの装着されていた端末が悪意ある第三者の手に渡ったとしても、その端末から情報が採取される恐れは極めて少ない。しかも、ＩＣカード自体を解析しようとして、ＩＣカードの回路を露出するためにＩＣカードの封止をとくと、回路自体が破壊される。このため、ＩＣカードの解析によってＩＣカードに記憶された情報が採取される可能性も極めて小さい。さらに、異なる通信事業者のＩＣカードが一つの端末に装着される場合でも、ＩＣカードに端末識別情報が記憶されるから、悪意ある第三者の手にその端末が渡っても、これらの情報が一度に危険にさらされる恐れはない。

【００２３】このＩＣカードには、端末識別情報とは別に要求情報の要求が正当であることを表す認証情報を記憶する認証情報記憶手段を備えてもよい。認証情報は、例えば（正当な）利用者が他者に対して秘匿しているパスワードなどである。バイオメトリクスなどの情報を認証情報として用いてもよい。

【００２４】許可決定手段は、端末識別情報が相違する場合に、装着された端末から入力された認証情報と認証情報記憶手段に記憶された認証情報とを比較する。そして、許可決定手段は、認証情報も相違したときにのみ要求情報の出力を禁止する。認証情報が一致したときには、要求情報の出力は許可される。

【００２５】ＩＣカードが組み合わされていたのとは別の端末を利用者が利用する場合、端末を介してＩＣカードに認証情報を入力すればよい。この認証情報の比較や記憶も、ＩＣカードで行われるから認証情報も確実に保護される。

【００２６】また、ＩＣカードの端末識別情報記憶手段には、例えば許可決定手段によって要求情報の出力が前回許可された端末の端末識別情報が記憶される。

【００２７】この場合に、ＩＣカードに端末識別情報更新手段を備えてもよい。端末識別情報更新手段は、認証情報が一致したとき、端末識別情報記憶手段に記憶された端末識別情報を装着された端末の端末識別情報に自動的に更新する。

【００２８】このため、以降端末が情報を要求しても、その際利用者が認証情報を入力する必要はなくなる。なお、これによって、それまでと異なる端末の端末識別情報に端末識別情報記憶手段に記憶された端末識別情報が更新されることになるが、元に戻すには、ＩＣカードを元の端末に装着して認証情報を一致させればよい。

【００２９】ＩＣカードにおいて、許可決定手段は、少なくとも要求情報が課金に利用される課金利用情報である場合、課金利用情報の出力を許可するか否かを決定する。この課金利用情報は、課金対象を特定する例えば利用者を識別するための利用者識別情報などである。課金利用情報がＩＣカードから端末に出力されなければ、少なくとも被害者が経済的被害を受けるのを抑止することができる。

【００３０】また、認証情報記憶手段は、認証情報だけでなく、電子商取引における認証に利用される取引用認証情報も記憶することがある。

【００３１】許可決定手段は、端末識別情報が相違する場合に、認証情報が一致したときでも、すぐさま要求情報の出力を許可しない。許可決定手段は、認証情報が一致したとき、装着された端末から入力された取引用認証情報と認証情報記憶手段に記憶された取引用認証情報とを比較する。そして、許可決定手段は、取引用認証情報も一致すれば課金利用情報の出力を許可する。

【００３２】電子商取引において利用者識別情報などが不正利用されると、特に利用者の被害が甚大になる恐れがあるが、取引用認証情報を用いた認証も行うことによって、このような被害をより確実に抑止することができる。

【００３３】また、ＩＣカードに暗号化手段を備えてもよい。この暗号化手段は、許可決定手段が装着された端末に要求情報を出力することを許可した場合に、装着された端末に出力される要求情報を暗号化する。

【００３４】この場合、要求情報の出力が許可されても、平文の要求情報はＩＣカードから端末に出力されないから、万一ＩＣカードの外部で要求情報が採取されたとしても、採取された要求情報の不正利用や漏洩の危険性を抑えることができる。

【００３５】また、ＩＣカードの端末識別情報記憶手段

には、予め定められた端末識別情報のみが記憶されることもある。この場合、端末識別情報記憶手段は、１つだけ端末識別情報を記憶してもよいし、端末識別情報を複数記憶してもよい。

【００３６】また、このようなＩＣカードが装着され、電気通信回線を通じて通信を行う好ましい通信端末では、自端末の端末識別情報が自端末識別情報記憶手段に記憶される。通信許可決定手段は、自端末識別情報記憶手段に記憶された自端末の端末識別情報を装着されたＩＣカードに出力し、自端末の端末識別情報に対する装着されたＩＣカードの許可決定手段による決定に従い、要求情報を利用する通信を許可するか禁止するかを決定する。

【００３７】要求情報を利用する通信には、例えば利用者識別情報によって識別される利用者に対して課金が発生するサービスにおける通信など、利用者識別情報自体の通信だけでなく、利用者識別情報とそれに関連する情報の通信も含まれる。

【００３８】ＩＣカードから要求情報が出力されなければ、要求情報を利用する通信はできないが、この通信端末は、その通信自体の許可又は禁止を決定することによって、要求情報を二重に保護する。

【００３９】また、上述のようなＩＣカードが取り外し可能に装着される各種の端末には、認証情報変更手段を備えてもよい。認証情報変更手段は、認証情報記憶手段の記憶内容を変更するために用いられる。変更される内容には、通常利用される認証情報や取引用認証情報が含まれる。認証情報変更手段は、ＩＣカード自体に備えることもできる。

【００４０】また、通信機器と電気通信回線を介して通信に利用される通信端末と、その通信端末に取り外し可能に装着され、通信端末との間で情報の入出力を行うＩＣカードとを備えた通信局において、出力暗号化手段は、そのＩＣカードに備えられ、通信端末に出力される利用者を識別するための利用者識別情報を暗号化するために用いられる。通信端末に備えられる自端末識別情報記憶手段には、その通信端末に対する端末を識別するための端末識別情報が記憶される。暗号化組合せ情報生成手段は、自端末識別情報記憶手段に記憶された通信端末の端末識別情報と利用者識別情報との組合せを表す組合せ情報の少なくとも利用者識別情報が出力暗号化手段によって暗号化された暗号化組合せ情報を生成する。通信許可決定手段は、通信端末によって暗号化組合せ情報が送信された通信機器から、通信端末が、暗号化組合せ情報から復元された組合せ情報が正当な組合せを表すことを証明する証明情報を受信した場合にのみ、利用者識別情報を利用する通信を許可するか禁止するかを決定する。

【００４１】この通信局では、ＩＣカードから通信端末に利用者識別情報が出力されるものの、その利用者識別情報は暗号化されている。このため、悪意ある第三者にＩＣカードから出力された利用者識別情報が採取されたとしても、その利用者識別情報が漏洩する恐れは小さくなる。また、組合せ情報が正当であるか否かは通信機器で比較され、通信端末は、組合せ情報が正当であると証明された場合に、利用者識別情報を利用する通信が許可されるから、悪意ある第三者は利用者識別情報を不正使用することができない。

【００４２】この通信局において、暗号化組合せ情報生成手段は、例えば通信端末に備えられ、自端末情報記憶手段に記憶された通信端末の端末識別情報とＩＣカードから通信端末に出力された暗号化された利用者識別情報とを用いて暗号化組合せ情報を生成する。

【００４３】また、暗号化組合せ情報生成手段は、ＩＣカードに備えられてもよい。この場合、暗号化組合せ情報生成手段は、通信端末からＩＣカードに入力された通信端末の端末識別情報と出力利用者識別情報暗号化手段によって暗号化された利用者識別情報とを用いて暗号化組合せ情報を生成する。

【００４４】また、出力暗号化手段には、利用者識別情報を記憶する利用者識別情報記憶手段と、利用者識別情報記憶手段に記憶された利用者識別情報を暗号化する利用者識別情報暗号化手段とを有することができる。

【００４５】出力暗号化手段は、例えば通信機器が復号化に利用する秘密鍵に対応する公開鍵を用いて暗号化組合せ情報を生成する。

【００４６】ここで、証明情報は、組合せ情報が正当なものであることが移動通信端末を移動体通信網に接続するための網接続装置によって証明されたものなどである。また、証明情報は、組合せ情報が正当なものであることが電子商取引を管理する電子商取引サーバによって証明されたものであってもよい。

【００４７】上述のような通信局と電気通信回線を介して通信を行う好ましい通信機器では、利用者識別情報と端末識別情報との組合せが組合せ記憶手段に記憶される。組合せ情報復元手段は、通信局によって送信された暗号化組合せ情報から組合せ情報を復元する。証明情報生成手段は、組合せ記憶手段に記憶された利用者識別情報と端末識別情報との組合せのうち、組合せ情報復元手段によって復元された組合せ情報が表す利用者識別情報と端末識別情報との組合せと一致する組合せがある場合に、組合せ情報が正当な組合せを表すことを証明する証明情報を生成する。

【００４８】また、上述のようなＩＣカードと、ＩＣカードが装着される通信端末とを備えた通信局では、通信端末を利用して行う通信を制御するために、ＩＣカードによって、ＩＣカードに記憶されている端末識別情報と通信端末からＩＣカードに入力された通信端末の端末識別情報とが比較される。続いて、端末識別情報の比較結果に基づいて、要求情報を通信端末に出力することを許

可するか禁止するかがＩＣカードによって決定される。そして、ＩＣカードから通信端末に要求情報が出力された場合にのみ、要求情報を利用する通信が通信端末によって行われる。

【００４９】他の通信局では、通信端末を利用して行う通信を制御するために、ＩＣカードから通信端末に出力される利用者を識別するための利用者識別情報が暗号化された暗号化利用者情報と通信端末に記憶されている通信端末の端末識別情報とを用いて、利用者識別情報と通信端末の端末識別情報との組合せを表す組合せ情報のうち少なくとも利用者識別情報が暗号化された暗号化組合せ情報が生成される。通信端末を用いて暗号化組合せ情報は通信機器に電気通信回線を介して送信される。そして、その通信機器から、通信端末が証明情報を受信した場合にのみ、利用者識別情報を利用する通信が行われる。

【００５０】

【発明の実施の形態】以下、添付図面を参照して本発明の実施の形態につき説明する。以下の実施の形態において、本発明は、移動通信システム又はその移動通信システムを含む通信システムを構成する機器やその一部として提供される。

【００５１】移動通信システムは、携帯電話機が他の携帯電話機などと通話やデータ通信を行うためのシステムである。移動通信システムは、移動局となる携帯電話機の他、基地局系装置、交換機などからなる。

【００５２】図２には、携帯電話機、基地局系装置、交換機の関係が簡略的に示されている。

【００５３】図２に示すように、基地局系装置１００には、基地局に設置される無線基地局装置１０１や移動交換局に設置される基地局制御装置１０２が含まれる。携帯電話機１０３は、無線基地局装置１０１に無線接続される。無線基地局装置１０１は、基地局制御装置１０２によって制御される。基地局制御装置１０２は、発着信の接続制御や基地局間でのチャンネル切替制御などの他、接続された各無線基地局装置１０１の運用管理にも用いられる。基地局制御装置１０２は、移動交換局に設置される交換機１０４によって基幹網に接続される。基幹網は、散在する交換機１０４やゲートウェイ交換機を結ぶATM(Asynchronous Transfer Mode)ネットワークなどで構築されている。移動通信システムの移動通信網は、これらの機器や基幹網によって提供される。

【００５４】携帯電話機１０３が他の通信機器と通信するために発信を行う場合、無線基地局装置１０１、基地局制御装置１０２を介して、発信要求を交換機１０４に送信する。交換機１０４は、発信要求が契約している正規の利用者によってなされたことを確認すると、ゲートウェイ交換機に回線設定要求を行う。ゲートウェイ交換機は、交換機１０４からの要求を受けて、携帯電話機１０３と他の携帯電話機などとを接続するための電気通信回線を移動通信網に設定する。携帯電話機１０３は、設定された電気通信回線を通じて他の携帯電話機などと通信を行う。

【００５５】発信要求には、利用者を識別するための利用者識別コードが含まれる。交換機１０４は、この利用者識別コードをもとに、正規の利用者であるか否かを確認する。また、交換機１０４は、回線の接続時間など課金に必要な課金情報を利用者識別コードに対応付けて、課金センターに送信する。これにより、携帯電話機を用いて通信を行うと、確認された利用者識別コードによって識別される利用者に対して課金が行われる。

【００５６】この実施の形態では、携帯電話機１０３は、発信要求を送信する際、ＩＣカードから利用者識別コードを取得する。

【００５７】図３は携帯電話機のハードウェア構成を簡略的に示す。

【００５８】図３に示すように、携帯電話機１０３は、移動通信端末１０５と、移動通信端末１０５に取り外し可能に装着されるＩＣカード１０６とを備える。

【００５９】移動通信端末１０５において、キー入力部１０５１は、移動通信端末１０５の筐体表面に設けられた例えば数字キーや電源キー、各種の機能キーである。利用者は、このキー入力部１０５１を用いて、電源の投入・切断を行ったり、数字や文字を入力したり、カーソルを動かしたりする。

【００６０】表示部１０５２には、液晶ディスプレイを用いることができる。表示部１０５２には、キー入力部１０５１から入力された数字や文字、移動通信端末１０５の動作設定を行うための設定画面などが表示される。

【００６１】メモリ部１０５３には、例えばＲＡＭとフラッシュメモリが含まれる。ＲＡＭは、ＣＰＵのワーク領域に用いられる。フラッシュメモリは、この移動通信端末１０５に固有の端末を識別するための端末識別コードや移動通信端末１０５の動作設定を表す情報などを保持しておくのに用いられる。

【００６２】音声入出力部１０５４は、マイクやスピーカである。音声入出力部１０５４は、利用者が通話したり、着信音を鳴らせたりするのに用いられる。

【００６３】通信部１０５５は、基地局と無線通信を行うためのアンテナや変調回路などの無線回路などである。

【００６４】インタフェース部１０５６は、移動通信端末１０５とＩＣカード１０６とが情報を入出力するのに用いられる。

【００６５】制御部１０５７には、例えばＣＰＵとＤＳＰが含まれる。制御部１０５７は、上述の各部と入出力を行って、移動通信端末１０５全体を制御する。制御部１０５７は、音声の符号化、復号化などの音声処理の他、アプリケーションの実行にも用いられる。

【００６６】また、ＩＣカード１０６において、不揮発

性メモリ部１０６１には、フラッシュメモリやＥＥＰＲＯＭ、その他の電気的に書き換え可能な不揮発性メモリが用いられる。不揮発性メモリ部１０６１は、利用者識別コードや利用者が登録した電話帳、通話履歴などの他の情報や、必要なアプリケーションを記憶する。

【００６７】インタフェース部１０６２は、例えばＩＣカード１０６の表面に設けられた所定形式のコンタクトピンを備える。このコンタクトピンを移動通信端末１０５のインタフェース部１０５６に接触させることによって、ＩＣカード１０６のインタフェース部１０６２と移動通信端末１０５のインタフェース部１０５６は取り外し可能に接続される。

【００６８】制御部１０６３は、インタフェース部１０６２及び不揮発性メモリ部１０６１の入出力を制御したり、暗号処理や暗号復号化処理を行ったり、ＯＳやＯＳ上で動作するアプリケーションを実行したりする。制御部１０６３には、ＣＰＵが用いられる。通常暗号処理のためにコプロセッサも備えられる。

【００６９】この携帯電話機１０３では、図２における破線で示すように、携帯電話機１０３の移動通信端末１０５からＩＣカード１０６を取り外し、取り外されたＩＣカード１０６を他の移動通信端末１０５に装着することも可能である。

（適用例１）この適用例１では、本発明は、移動通信端末１０５若しくはＩＣカード１０６又は携帯電話機１０３に適用される。

＜ＩＣカード＞この適用例１において、本発明が適用されたＩＣカード１０６は、移動通信端末１０５が交換機１０４に発信要求を送信するために、不揮発性メモリ部１０６１に記憶された利用者識別コードを要求しても、その要求が正当なものでなければ、利用者識別コードを出力しない。

【００７０】例えばこの制御を行うための制御プログラムをＩＣカード１０６の制御部１０６３に実行させることによって、上述のＩＣカード１０６は、本発明が適用されたＩＣカードとして機能する。

【００７１】この場合、図１に示すように、ＩＣカード１０６の制御部１０６３は、許可決定手段１として動作し、不揮発性メモリ部１０６１（の一部領域）は、端末識別情報記憶手段２として用いられる。

【００７２】端末識別情報記憶手段２は、端末識別コードを記憶する。この端末識別コードは、例えば通信事業者に申し出た利用者の移動通信端末１０５と同じ端末識別コードを、通信事業者が予め登録したものである。利用者が複数の移動通信端末１０５を利用する場合には、端末識別情報記憶手段２に、複数の端末識別コードを記憶してもよい。

【００７３】許可決定手段１は、比較手段３と決定手段４とを有する。比較手段３は、装着された移動通信端末１０５からインタフェース部１０６２を介して入力された端末識別コードと端末識別情報記憶手段２に記憶された端末識別コードとを比較する。端末識別情報記憶手段２に複数の端末識別コードが記憶されている場合には、比較手段３は、記憶された全ての端末識別コードと入力された端末識別コードを比較する。

【００７４】決定手段４は、比較手段３による比較結果に基づいて、装着された移動通信端末１０５が要求する利用者識別コードを装着された移動通信端末１０５に出力することを許可するか禁止するかを決定する。

【００７５】ここで、図４はこのＩＣカードを備えた携帯電話機による通信制御方法を説明するためのフローチャートである。

【００７６】図４に示すように、移動通信端末１０５から利用者識別コードを要求するコマンドが受信されると（Ｓ４０１）、比較手段３は、端末識別コードの比較を行う（Ｓ４０２）。コマンドには、移動通信端末１０５のメモリ部１０５３に記憶された端末識別コードが含まれており、比較手段３は、この端末識別コードをコマンドから取得する。また、比較手段３は、端末識別情報記憶手段２から端末識別コードを読み出す。比較手段３は、移動通信端末１０５から入力された端末識別コードを端末識別記憶手段２から読み出された端末識別コードと比較し、比較結果を決定手段４に出力する。

【００７７】移動通信端末１０５から入力された端末識別コードが、端末識別情報記憶手段２から読み出された端末識別コードのいずれかに一致する場合、決定手段４は、不揮発性メモリ部１０６１に記憶された利用者識別コードを、装着された移動通信端末１０５に出力することを許可する決定を行う。この場合、移動通信端末１０５からのコマンドに対して、利用者識別コードを含む応答データが作成される（Ｓ４０３）。

【００７８】また、移動通信端末１０５から入力された端末識別コードが端末識別情報記憶手段２から読み出された端末識別コードのいずれにも相違する場合、決定手段４は、不揮発性メモリ部１０６１に記憶された利用者識別コードを、装着された移動通信端末１０５に出力することを禁止する決定を行う。この場合、移動通信端末１０５からのコマンドに対して、エラーを表す応答データが作成される（Ｓ４０４）。

【００７９】手順Ｓ４０３又はＳ４０４において作成された応答データは、ＩＣカード１０６からインタフェース部１０６２を通じて移動通信端末１０５に送信される。

【００８０】このように、このＩＣカード１０６では、端末識別コードが相違する場合に、利用者識別コードが移動通信端末１０５に出力されない。ＩＣカード１０６が紛失や盗難によって、本来の利用者とは別の悪意ある第三者の手に渡った場合、その第三者は、利用者が利用していた移動通信端末１０５とは異なる端末にＩＣカード１０６を装着することになる。従って、ＩＣカード１

０６に記憶された利用者識別コードは、悪意ある第三者の移動通信端末に出力されない。

【００８１】この場合、移動通信端末は、利用者識別コードを取得できないから、その利用者識別コードを用いて発信要求を行うこともできない。その結果、ＩＣカード（の利用者識別コード）の不正利用を防止することができる。また、ＩＣカードが装着された他の端末を解析しても、要求情報がその端末に出力されないから、端末からそれらを採取することもできない。さらに、端末にＩＣカードに関する情報を記憶する必要がないので、ＩＣカードの装着されていた端末が悪意ある第三者の手に渡ったとしても、その端末から情報が採取される恐れは極めて少ない。しかも、ＩＣカード自体を解析しようとして、ＩＣカードの回路を露出するためにＩＣカードの封止をとくと、回路自体が破壊される。このため、ＩＣカードの解析によってＩＣカードに記憶された情報が採取される可能性も極めて小さい。さらに、異なる通信事業者のＩＣカードが一つの端末に装着される場合でも、ＩＣカードに端末識別情報が記憶されるから、悪意ある第三者の手にその端末が渡っても、これらの情報が一度に危険にさらされる恐れはない。

【００８２】なお、例えばＩＣカード１０６の不揮発性メモリ部１０６１に通信履歴や電話帳、電子商取引の取引明細などの個人情報が記憶されている場合、この個人情報が漏洩すると、それによって、利用者が経済的、精神的な被害を受ける恐れがある。このため、移動通信端末１０５がＩＣカード１０６に個人情報などを要求した場合にも、許可決定手段１が、利用者識別コードと同様に、移動通信端末１０５がＩＣカード１０６に要求した要求情報をその移動通信端末１０５に出力することを許可するか禁止するかを決定するようにしてもよい。

【００８３】また、ＩＣカード１０６には、図５に示すように、暗号化手段５を備えてもよい。この暗号化手段５は、例えば許可決定手段１によって移動通信端末１０５への出力が許可された利用者識別コードを暗号化する。この場合、移動通信端末１０５には、暗号化手段５によって暗号化された利用者識別コードを含む応答データが送信される。もちろん、暗号化手段５によって、利用者識別コードだけでなく、移動通信端末１０５に出力する他の情報も暗号化するようにしてもよい。

【００８４】このようにＩＣカードから移動通信端末に暗号化された利用者識別コードを出力することによって、悪意ある第三者によって平文の利用者識別コードが移動通信端末から採取される可能性をさらに抑えることができる。

【００８５】＜移動通信端末＞移動通信端末１０５は、上述のＩＣカード１０６の制御に対応する制御プログラムを制御部１０５７に実行させることによって、本発明が適用された移動通信端末１０５として機能する。

【００８６】この場合、移動通信端末１０５では、図６に示すように、制御部１０５７は通信許可決定手段６として動作し、メモリ部１０５３（の一部領域）は自端末識別情報記憶手段７として用いられる。

【００８７】自端末識別情報記憶手段７は、この移動通信端末１０５に固有の端末識別コードを記憶する。通信許可決定手段６は、装着されたＩＣカード１０６に自端末の端末識別コードを出力し、自端末の端末識別コードに対するＩＣカード１０６の許可決定手段１による決定に従い、利用者識別コードを用いた発信要求を行うことを許可するか禁止するかを決定する。

【００８８】図７はこの移動通信端末とＩＣカードの動作の関係を説明するためのフローチャートである。

【００８９】図７に示すように、移動通信端末１０５は、交換機１０４に発信要求を行う場合に、自端末識別情報記憶手段７から自端末の端末識別コードを読み出し、この端末識別コードを含み、利用者識別コードを要求するコマンドを作成する（Ｓ７０１）。

【００９０】移動通信端末１０５は、作成されたコマンドを、インタフェース部１０５６を介してＩＣカード１０６に送信する（Ｓ７０２）。ＩＣカード１０６がコマンドを受信すると、既に説明した手順Ｓ４０１乃至Ｓ４０５に従い、ＩＣカード１０６から移動通信端末１０５にコマンドに対する応答データが送信される。

【００９１】移動通信端末１０５がＩＣカード１０６からの応答データを受信すると（Ｓ７０３）、通信許可決定手段６は、応答データが利用者識別コードを含むものであるかエラーを表すものであるかを判断する（Ｓ７０４）。

【００９２】通信許可決定手段６は、応答データが利用者識別コードを含むものであると判断した場合、通信を許可する決定を行う（Ｓ７０５）。この場合、応答データに含まれる利用者識別コードを用いて発信要求が生成され、移動通信端末１０３から無線基地局１０１を経由して交換機１０４に発信要求が送信される。一方、応答データがエラーを表すものであると判断された場合、通信許可決定手段６は、通信を禁止する決定を行う（Ｓ７０６）。移動通信端末１０５は、必要に応じて、表示部１０５２に端末識別コードが相違する旨のメッセージを表示するが、発信要求は送信しない。

【００９３】なお、この適用例１では、移動通信端末について本発明を適用したが、ＩＣカードが取り外し可能に装着されるPDAやその他の端末などにも本発明を適用することが可能である。この端末には、通信を行う通信端末だけでなく、通信を自身で行わない端末も含まれる。通信を行わない端末でもその表示部に要求情報が表示されることによって、要求情報が漏洩するなどの危険性がある。

（適用例１の変形例１）適用例１では、端末識別情報記憶手段２に端末識別コードが予め登録されていない移動通信端末１０５に装着されると、その移動通信端末１０

５は、利用識別コードを取得することができなかった。

【００９４】ただし、利用者が新しい端末を購入した場合などにも、登録されていない移動通信端末１０５にＩＣカード１０６が装着される可能性がある。この場合に、通信事業者に、新しい移動通信端末の端末識別コードを端末識別情報記憶手段２に登録することを依頼するのは、利用者にとって不便である。

【００９５】そこで、図８に示すように、ＩＣカード１０６の不揮発性メモリ部１０６１を端末識別情報記憶手段２としてだけでなく、認証情報記憶手段８としても用いるようにする。

【００９６】認証情報記憶手段８は、認証コードを記憶する。認証コードは、端末識別コードとは別に、利用者識別情報の要求が正当であることを表すパスワードやバイオメトリクスの情報である。

【００９７】許可決定手段１は、端末識別コードが相違する場合に、装着された移動通信端末１０５から入力された認証コードと認証情報記憶手段８に記憶された認証コードとを比較し、認証コードも相違したときにのみ利用者識別コードの出力を禁止する。

【００９８】図９は、認証コードを利用する場合の移動通信端末とＩＣカードの動作の関係を説明するためのフローチャートである。

【００９９】端末識別コードが一致する場合、既に説明した通りの手順Ｓ４０３、Ｓ４０５が行われるが、この例では、端末識別コードが相違する場合に、許可決定手段１は、すぐさま利用者識別コードの出力を禁止しない。例えば端末識別コードが相違する場合、比較手段３は決定手段４に比較結果を出力せず、移動通信端末１０５に端末識別コードが相違する旨を通知する。

【０１００】移動通信端末１０５は、この通知を受けると、図９に示すように、例えばメモリ部１０５３に記憶されたパスワードを要求する画面を表示部１０５２に表示する（Ｓ９０１）。

【０１０１】そして、利用者がキー入力部１０５１を用いてパスワードを入力すると、移動通信端末１０５は、パスワードの入力を受け付け（Ｓ９０２）、受け付けたパスワードを含む認証要求コマンドを作成し、ＩＣカード１０６に送信する（Ｓ９０３）。

【０１０２】ＩＣカード１０６が認証要求コマンドを受信すると（Ｓ９０４）、比較手段３は、認証要求コマンドからパスワードを取得する。また、比較手段３は、認証情報記憶手段８からパスワードを読み出し、読み出されたパスワードを移動通信端末１０５から入力されたパスワードと認証情報記憶手段８から読み出したパスワードと比較し（Ｓ９０５）、比較結果を決定手段４に出力する。

【０１０３】決定手段４は、比較結果がパスワードも相違することを表す場合、利用者識別コードを移動通信端末１０５に出力することを禁止する決定を行う。この場合、エラーを表す応答データが作成される（Ｓ４０４）。このため、パスワードを知らない第三者は、利用者識別コードをＩＣカード１０６から取得することができない。

【０１０４】これに対し、比較結果がパスワードは一致することを表す場合、決定手段４は、利用者識別コードを移動通信端末１０５に出力することを許可する決定を行う。この場合、上述のＩＣカードと同様に、利用者識別コードを含む応答データが作成される（Ｓ４０３）。

【０１０５】作成された応答データは、移動通信端末１０５に送信され（Ｓ４０５）、既に説明した手順Ｓ７０３乃至Ｓ７０６の通り、移動通信端末１０５で通信を許可するか禁止するかが決定される。

【０１０６】このように、ＩＣカードに認証情報記憶手段８を備えておけば、利用者が新しい移動通信端末を購入した場合などでも、その新しい移動通信端末でＩＣカードに記憶された利用者識別コードを利用することができる。

【０１０７】なお、この例では、次に発信要求を行う場合にも、パスワードの入力が求められてしまう。このため、図１０に示すように、ＩＣカード１０６の制御部１０６３を端末識別情報更新手段９としても動作させるのが好ましい。

【０１０８】端末識別情報更新手段９は、パスワードが一致することを表す比較結果が許可決定手段１から入力されると、図９において破線で示す手順Ｓ９０６の通り、端末識別情報記憶手段２に記憶された端末識別コードを、移動通信端末１０５から入力された端末識別コードに更新する。

【０１０９】この場合、端末識別情報記憶手段２には、許可決定手段１によって利用者識別コードの出力が前回許可された端末の端末識別コードが記憶されることになる。

【０１１０】これによって、利用者識別コードが次に要求された場合には、端末識別コードが一致することになるから、パスワードの入力は求められない。

【０１１１】また、悪意ある第三者が携帯電話機１０３を用いて通話するだけでなく、他人の利用者識別コードを不正利用して電子商取引を行う場合には、その利用者の被害はさらに甚大になる恐れがある。このため、少なくとも要求情報が利用者識別コードなど課金に利用される課金利用情報である場合には、許可決定手段１によって、課金利用情報の出力を許可するか禁止するかを決定するのが好ましい。課金利用情報の出力を制御していれば、少なくとも利用者が被る経済的被害を抑制することができる。

【０１１２】そして、認証情報記憶手段８に、通常の認証コードだけでなく、電子商取引における認証に利用される取引用認証情報も記憶しておき、これを用いた認証も行う。

【０１１３】この場合、端末識別コードが相違して認証コードも相違するならば、上述したのと同じ手順Ｓ４０４、Ｓ４０５が行われるが、認証コードが一致するときでも、許可決定手段１は、すぐさま利用者識別コードの出力を許可する決定を行わない。認証コードが一致しても、例えば比較手段３は、比較結果を決定手段４に出力せず、認証コードが一致した旨を移動通信端末１０５に通知する。移動通信端末１０５がこの通知を受けた以降の手順は、図９における認証コードを取引用認証コードに置き替えた手順になる。

【０１１４】すなわち、移動通信端末１０５は通知を受けると、例えばメモリ部１０５３に記憶された電子商取引用のパスワードを要求する画面を表示部１０５２に表示する。

【０１１５】そして、利用者によりキー入力部１０５１を用いて電子商取引用のパスワードが入力されると、移動通信端末１０５は、そのパスワードの入力を受け付け、電子商取引用のパスワードを含む認証要求コマンドを生成し、ＩＣカード１０６に送信する。

【０１１６】ＩＣカード１０６が認証要求コマンドを受信すると、比較手段３は、認証要求コマンドから電子商取引用のパスワードを取得する。また、比較手段３は、認証情報記憶手段８から電子商取引用のパスワードを読み出し、移動通信端末１０５から入力された電子商取引用のパスワードと認証情報記憶手段８から読み出した電子商取引用のパスワードとを比較し、比較結果を決定手段４に出力する。

【０１１７】決定手段４は、比較結果は電子商取引用のパスワードが相違することを表す場合、通常のパスワードが一致していても、利用者識別コードを移動通信端末１０５に出力することを禁止する決定を行う。この場合、エラーを表す応答データが作成される。このため、パスワードを知っていたとしても電子商取引用パスワードを知らなければ、第三者は、利用者識別コードを利用して電子商取引を行うことができない。

【０１１８】これに対し、比較結果は電子商取引用のパスワードが一致することを表す場合、決定手段４は、利用者識別コードを移動通信端末１０５に出力することを許可する決定を行う。この場合、上述のＩＣカード１０６と同様に、利用者識別コードを含む応答データが作成される。

【０１１９】作成された応答データは、移動通信端末１０５に送信され、移動通信端末１０５で通信を許可するか禁止するかが決定される。

【０１２０】このように、認証情報記憶手段８に通常の認証コードだけでなく取引用認証コードも記憶しておけば、悪意ある第三者が利用者の識別コードを不正に利用して電子商取引を行うことによって利用者が経済的被害を受ける可能性をさらに抑えることができる。

（適用例１の変形例２）また、上述のように認証コードや取引用認証コードを用いる場合、常に同じものを用いていると、それらの認証コードが悪意ある第三者によって特定される可能性が高まる。このため、例えば移動通信端末１０５の制御部１０５７にプログラムを実行させ、図１１に示すように、制御部１０５７を認証情報変更手段１０として動作させるようにしてもよい。

【０１２１】認証情報変更手段１０は、利用者の指示に従い、認証情報記憶手段８に記憶された認証コードや取引用認証コードなどの記憶内容を変更するための制御を行う。

【０１２２】利用者は、パスワードを変更する場合、キー入力部１０５１を用いてその旨を指示すると、認証情報変更手段１０は、図１２に示すように、これまで利用されていた前パスワードの入力を求める画面を表示部１０５２に表示させる（Ｓ１２０１）。利用者によって前パスワードが入力され、認証情報変更手段１０が受け付けると（Ｓ１２０２）、認証情報変更手段１０は、受け付けた前パスワードの照合を要求する照合要求コマンドを生成する。この照合要求コマンドは移動通信端末１０５からＩＣカード１０６に送信される（Ｓ１２０３）。

【０１２３】ＩＣカード１０６が移動通信端末１０５から照合要求コマンドを受信すると（Ｓ１２０４）、比較手段３は、照合要求コマンドから前パスワードを取得し、認証情報記憶手段８に記憶されているパスワードと比較する（Ｓ１２０５）。比較結果が、一致することを表す場合にも、相違することを表す場合にも、それぞれ照合要求コマンドに対して、この比較結果を含む応答データが作成され（Ｓ１２０６、Ｓ１２０７）、ＩＣカード１０６から移動通信端末１０５に応答データが送信される（Ｓ１２０８）。

【０１２４】移動通信端末１０５がこの応答データを受信すると（Ｓ１２０９）、認証情報変更手段１０は、応答データから比較結果を取得する（Ｓ１２１０）。比較結果が相違する場合、パスワードを変更する処理は終了する。

【０１２５】また、比較結果が一致することを表す場合、認証情報変更手段１０は、新しいパスワードの入力を求める画面を表示部１０５２に表示する（Ｓ１２１１）。利用者がキー入力部１０５１を用いて新しいパスワードを入力し、認証情報変更手段１０がこれを受け付けると（Ｓ１２１２）、受け付けた新パスワードに前パスワードを更新することを要求する変更要求コマンドが生成される。変更要求コマンドは、前パスワードと新パスワードとを含み、ＩＣカード１０６に送信される（Ｓ１２１３）。

【０１２６】ＩＣカード１０６は、この変更要求コマンドを受信すると（Ｓ１２１４）、変更要求コマンドから前パスワードと新パスワードを取得する。比較手段３は、取得された前パスワードと認証情報記憶手段８に記憶されているパスワードと比較する（Ｓ１２１５）。比

較結果が、一致することを表す場合、ＩＣカード１０６は、取得された新しいパスワードに認証情報記憶手段８に記憶された前パスワードを更新する（Ｓ１２１６）。

【０１２７】パスワードは、例えばこのような手順で変更される。これによって、認証コードや取引用認証コードが特定される危険性が抑えられ、その結果、利用者識別コードなどの情報が不正利用されたり、漏洩したりする恐れが抑制される。この例のように、通信を行う度に、変更前の認証コードや取引用認証コードを認証情報記憶手段に記憶されたものと比較すれば、それらの変更はより安全に行われる。

【０１２８】また、この例では、移動通信端末１０５の制御部１０５７を認証情報変更手段１０として動作させたが、例えばＩＣカード１０６の制御部１０６３を認証情報変更手段として動作させることによって、ＩＣカード１０６に認証情報変更手段を備えてもよい。この場合、移動通信端末１０５は、単にＩＣカード１０６の入力手段や表示手段として用いられ、認証コードや取引用認証コードの変更は、ＩＣカード１０６の認証情報変更手段の制御に従って行われることになる。また、例えばＩＣカード１０６自体に認証コード又は取引用認証コードの入力を行うための入力部や各種のメッセージを表示する表示部を設けてもよい。ＩＣカード１０６に入力部や表示部が設けられていれば、もちろん要求コマンドや応答データが送受信される必要はなくなる。また、通信の度に変更前の認証コードや取引用認証コードが比較される必要もない。

（適用例１の変形例３）変形例１では、認証コードが一致すれば、端末識別情報記憶手段２に記憶された端末識別コードは、端末識別情報更新手段９によって移動通信端末１０５から入力された端末識別コードに更新された。この場合、端末識別コードの更新には、認証コードが必要になるが、端末識別情報記憶手段２に端末識別コードが記憶されている移動通信端末５を用いることによって、端末識別コードの更新を安全に行うことも可能である。

【０１２９】この場合、ＩＣカード１０６の制御部１０６３は、移動通信端末１０５から入力された端末識別コードが端末識別情報記憶手段２に記憶された端末識別コードと相違すると、移動通信端末１０５から入力された端末識別コードを端末識別情報記憶手段２に記憶する。

【０１３０】端末識別情報記憶手段２には、例えば端末識別コードが２つまで記憶されるが、許可決定手段１は、端末識別情報記憶手段２に端末識別コードが２つ記憶されている間、利用者識別コードを移動通信端末１０５に出力することを許可する決定を行わない。

【０１３１】また、ＩＣカード１０６の制御部１０６３は、端末識別情報記憶手段２に２つの端末識別コードが記憶されている間、移動通信端末１０５が入力された端末識別コードが端末識別情報記憶手段２に記憶された端末識別コードに一致すれば、一致した端末識別コードを端末識別情報記憶手段２から消去する。

【０１３２】例えば利用者が新しい移動通信端末１０５を購入したために利用する端末を変更する場合、まず利用者はこれまでの移動通信端末１０５からＩＣカード１０６を取り外す。この状態では、端末識別情報記憶手段２に一つだけ端末識別コードが記憶されている。

【０１３３】次に、利用者は、取り外したＩＣカードを新しい移動通信端末１０５に装着し、その移動通信端末１０５に端末の変更を指示する。移動通信端末１０５の制御部１０５７は、利用者の指示に従い、新しい移動通信端末１０５の端末識別コードの照合を要求する照合要求コマンドを生成し、ＩＣカード１０６に送信する。

【０１３４】ＩＣカード１０６がこの照合要求コマンドを受信すると、比較手段３は、新しい移動通信端末から入力された端末識別コードと端末識別情報記憶手段２に記憶された端末識別コードとを比較する。

【０１３５】利用者によってＩＣカード１０６が新しい移動通信端末１０５に装着された場合でも、悪意ある第三者によってＩＣカード１０６がその第三者の移動通信端末１０５に装着された場合でも、比較結果は、端末識別コードが相違することを表すことになる。

【０１３６】比較結果が端末識別コードは相違することを表す場合、ＩＣカード１０６の制御部１０６３は、新しい移動通信端末１０５から入力された（端末識別情報記憶手段２に記憶されたものとは相違する）端末識別コードを端末識別情報記憶手段２に記憶する。

【０１３７】これによって、端末識別情報記憶手段２に２つの端末識別コードが記憶される。端末識別情報記憶手段２に２つの端末識別コードが記憶されると、ＩＣカード１０６の制御部１０６３は、エラーを表す応答データを作成し、作成した応答データを移動通信端末１０５に送信する。

【０１３８】移動通信端末１０５がこの応答データを受信すると、移動通信端末１０５は端末識別コードが相違する旨のメッセージを表示部１０５２に表示する。

【０１３９】次に、利用者は、ＩＣカード１０６を新しい移動通信端末１０５から取り外し、取り外されたＩＣカード１０６をこれまで利用していた移動通信端末１０５に装着する。これまでの移動通信端末１０５に対して、利用者が端末識別コードを消去する指示を行うと、移動通信端末１０５の制御部１０５７は、自端末の端末識別コードを含む消去要求を生成し、生成された消去要求をＩＣカード１０６に送信する。

【０１４０】ＩＣカード１０６が消去要求を受信すると、比較手段３は、消去要求から端末識別コードを取得し、取得された端末識別コードと端末識別情報記憶手段２に記憶された２つの端末識別コードとを比較する。比較手段３の比較結果が、取得された端末識別コードと端末識別情報記憶手段２に記憶された端末識別コードは一

致することを表す場合、制御部１０６３は、一致する端末識別コードを端末識別情報記憶手段２から消去する。

【０１４１】ＩＣカード１０６がこれまで利用されていた移動通信端末１０５に装着されていれば、端末識別コードは一致するから、一致する端末識別コードは消去され、端末識別情報記憶手段２には、新しい移動通信端末１０５の端末識別コードだけが記憶されることになる。

【０１４２】制御部１０６３は、消去が完了したことを表す応答データを作成し、移動通信端末１０５に応答データを送信する。移動通信端末１０５がこの応答データを受信すると、制御部１０５７は、端末識別コードが更新されたこと（又は端末識別コードの消去が完了したこと）を知らせるメッセージを表示部１０５２に表示する。

【０１４３】以降、利用者は、新しい移動通信端末１０５でＩＣカード１０６を利用することができる。利用できる移動通信端末１０５を元に戻すには、新しい移動通信端末１０５とこれまでの移動通信端末１０５を置き替えた作業を利用者が行えばよい。また、端末識別情報記憶手段２に新しい移動通信端末１０５とこれまでの移動通信端末１０５の端末識別コードが記憶されている状態で、これまでの移動通信端末１０５でＩＣカード１０６が利用できるようにするには、新しい移動通信端末１０５で端末識別コードの消去を行えばよい。

【０１４４】これに対し、比較手段３の比較結果が、取得された端末識別コードと端末識別情報記憶手段２に記憶された端末識別コードは相違することを表す場合、制御部１０６３は、端末識別情報記憶手段２に記憶された端末識別コードを消去しない。制御部１０６３は、エラーを表す応答データを作成し、その応答データを移動通信端末１０５に送信する。移動通信端末１０５がこの応答データを受信すると、制御部１０５７は、端末識別コードの更新にエラーが生じたことを知らせるメッセージを表示する。

【０１４５】紛失や盗難によって、ＩＣカード１０６だけが悪意ある第三者の手に渡った場合、ＩＣカード１０６は利用者のものとは異なる第三者の移動通信端末１０５に装着されることになる。この場合、端末識別情報記憶手段２に記憶された２つの端末識別コードがいずれも消去されないか、第三者の移動通信端末１０５の端末識別コードだけが消去される。このため、第三者は、ＩＣカード１０６を不正使用できず、端末識別コードの更新を行うこともできない。

【０１４６】なお、このような端末識別コードの更新では、認証コードは必ずしも必要ないが、認証コードと組み合わせることは可能である。例えば利用者が端末識別コードの消去を指示した場合に、認証コードの入力を求める。そして、入力された認証コードが認証情報記憶手段８に記憶されたものと一致し、端末識別コードも一致する場合に、制御部１０６３は、端末識別情報記憶手段２に記憶された端末識別コードを消去する。

（適用例２）適用例１では、ＩＣカード１０６が利用者識別コードの出力を制御することによって利用者識別コードの不正利用や漏洩が抑制されていた。この場合、移動通信端末１０５内の回路や信号が解析されたとしても、その移動通信端末１０５には、利用者識別コードが出力されないので、利用者識別コードが移動通信端末１０５の解析によって悪意ある第三者に採取される可能性は極めて少ない。また、ＩＣカード１０６を解析しようとしても、ＩＣカード１０６の封止をとくと、ＩＣカード１０６の回路自体が破壊されてしまうので、そこから利用者識別コードが採取される危険性は極めて小さい。

【０１４７】もっとも、利用者識別コードが暗号化されており、それが移動通信端末１０５内で比較などのために復号化されなければ、移動通信端末１０５から平文の利用者識別コードが採取される可能性は抑えられる。また、発信要求が契約している正規の利用者によってなされたことを確認するには、例えば交換機１０４で、平文の利用者識別コードが得られればよい。

【０１４８】このため、この適用例２では、携帯電話機１０３を構成するＩＣカード１０６に出力暗号化手段１１が備えられる。出力暗号化手段１１は、移動通信端末１０５に出力される利用者識別コードを暗号化する。この出力暗号化手段１１を実現するために、例えば図１３に示すように、ＩＣカード１０６の制御部１０６３は、制御プログラムに従い、利用者識別情報暗号化手段１２として動作する。また、ＩＣカード１０６の不揮発性メモリ部１０６１（の一部領域）は、利用者識別情報記憶手段１３として用いられる。

【０１４９】利用者識別情報記憶手段１３は、平文の利用者識別コードを記憶する。また、利用者識別情報暗号化手段１２は、利用者識別情報記憶手段１３に記憶された利用者識別コードを暗号化する。この暗号化には、移動通信端末１０５が発信要求を送信する交換機１０４が復号化するのに利用する秘密鍵に対応する公開鍵を用いることができる。

【０１５０】利用者識別コードが暗号化された暗号化利用者識別コードは、インタフェース部１０６２を介して移動通信端末１０５に出力される。

【０１５１】また、携帯電話機１０３を構成する移動通信端末１０５のメモリ部１０５３（の一部領域）は、自端末識別情報記憶手段１４として用いられる。この自端末識別情報記憶手段１４も、自端末識別情報記憶手段７と同様に、移動通信端末１０５に固有の端末識別コードを記憶する。

【０１５２】さらに、移動通信端末１０５の制御部１０５７は、暗号化組合せ情報生成手段１５及び通信許可決定手段１６として動作する。

【０１５３】暗号化組合せ情報生成手段１５は、暗号化組合せ情報を生成する。この暗号化組合せ情報は、自端

末識別情報記憶手段１４に記憶された移動通信端末１０５の端末識別コードと利用者識別コードとの組合せを表す組合せ情報の少なくとも利用者識別コードが出力暗号化手段１１によって暗号化された情報である。

【０１５４】ここでは、暗号化組合せ情報生成手段１５は、ＩＣカード１０６から入力された暗号化利用者識別コードと自端末識別情報記憶手段１４に記憶された自端末の端末識別コードとを結合して、暗号化組合せ情報を生成する。

【０１５５】通信許可決定手段１６は、移動通信端末１０５によって暗号化組合せ情報が送信された交換機から、移動通信端末１０５が、暗号化組合せ情報から復元された組合せ情報が正当な組合せを表すことを証明する応答データを受信した場合にのみ、利用者識別コードを利用した発信要求を行うことを許可する。

【０１５６】また、上述のような携帯電話機１０３と対応する交換機１０４には、図１４に示すように、組合せ記憶手段１７が備えられる。図１５に、組合せ記憶手段の記憶内容を示す。図１５に示すように、この組合せ記憶手段１７には、例えば通信事業者と契約している利用者の利用者識別コードとその利用者が利用している端末識別コードとの組合せが記憶される。

【０１５７】組合せ情報復元手段１８は、携帯電話機１０３によって交換機１０４に送信された暗号化組合せ情報から組合せ情報を復元する。暗号化組合せ情報が暗号化利用者識別コードと平文の端末識別コードとを結合することによって構成されている場合、組合せ情報復元手段１８は、暗号化利用者識別コードを上述の秘密鍵を用いて復号化して利用者識別コードを復元する。これによって、利用者識別コードと端末識別コードとの組合せを表す組合せ情報が復元される。

【０１５８】証明情報生成手段１９は、組合せ記憶手段１７に記憶された利用者識別コードと端末識別コードとの組合せのうち、組合せ情報復元手段１８によって復元された組合せ情報が表す利用者識別コードと端末識別コードとの組合せと一致する組合せがある場合に、その組合せ情報が正当な組合せを表すことを証明するデータを生成する。

【０１５９】図１６はこのような交換機と通信を行う携帯電話機による通信制御方法を説明するためのフローチャートである。

【０１６０】利用者がキー入力部１０５１を用いて発信を指示すると、移動通信端末１０５の制御部１０５７は、ＩＣカード１０６に利用者識別コードを要求するコマンドを生成し、ＩＣカード１０６に送信する。ＩＣカード１０６がこのコマンドを受信すると、利用者識別情報暗号化手段１２は、利用者識別情報記憶手段１３から利用者識別コードを読み出し、利用者識別コードを暗号化する。出力暗号化手段１１によって暗号化利用者識別コードが生成されると（Ｓ１６０１）、ＩＣカード１０６は暗号化利用者識別コードを含む応答データを作成し、作成された応答データを移動通信端末１０５に送信する。

【０１６１】移動通信端末１０５が応答データを受信すると、暗号化組合せ情報生成手段１５は、応答データから暗号化利用者識別コードを取得する。また、暗号化組合せ情報生成手段１５は、自端末識別情報記憶手段１４から自端末の端末識別コードを読み出し、読み出された端末識別コードと暗号化利用者識別コードとを結合して暗号化組合せ情報を生成する（Ｓ１６０２）。暗号化組合せ情報が生成されると、移動通信端末１０５は、生成された暗号化組合せ情報を含む認証要求を作成し、通信部１０５５を用いて無線基地局装置１０１に認証要求を送信する（Ｓ１６０３）。発信要求は無線基地局装置１０１を経由して交換機１０４に転送される。

【０１６２】交換機１０４が移動通信端末１０５からの認証要求を受信すると（Ｓ１６０４）、交換機１０４の組合せ情報復元手段１８は、認証要求から暗号化組合せ情報を取得し、暗号化組合せ情報の暗号化利用者識別コードを復号化することによって、組合せ情報を復元する（Ｓ１６０５）。

【０１６３】組合せ情報が復元されると、証明情報生成手段１９は、復元された組合せ情報が表す利用者識別コードと端末識別コードとの組合せと一致する組合せが組合せ記憶手段１７に記憶されているか否かを判定する（Ｓ１６０６）。

【０１６４】一致する組合せがあると判定された場合、証明情報生成手段１９は、組合せ情報が正当な組合せを表すことを証明する応答データを作成する（Ｓ１６０７）。

【０１６５】これに対し、一致する組合せがないと判定された場合、証明情報生成手段１９は、組合せ情報が正当な組合せを表さないことを示す応答データを作成する（Ｓ１６０８）。

【０１６６】手順Ｓ１６０７又はＳ１６０８において作成された応答データは、交換機１０４から無線基地局を経由して移動通信端末１０５に送信される。

【０１６７】移動通信端末１０５が発信要求に対する応答データを受信すると（Ｓ１６１０）、通信許可決定手段１６は、応答データは組合せ情報が正当な組合せを表すことを証明しているか否かを判定する（Ｓ１６１１）。

【０１６８】応答データは組合せ情報が正当な組合せを表すことを証明していると判定された場合、通信許可決定手段１６は、認証要求を行った利用者識別コードを利用した通信のために、発信要求を行うことを許可する。移動通信端末１０５が発信要求を無線基地局にすることによって、他の携帯電話機などへの電気通信回線が設定され、通信が開始される（Ｓ１６１２）。

【０１６９】また、応答データは組合せ情報が正当な組

合せを表すことを証明していないと判定された場合、通信許可決定手段１６は、発信要求を行うことを禁止し、禁止した旨を表示部１０５２に表示させる（Ｓ１６１３）。

【０１７０】なお、この例では、通信局として携帯電話機を説明したがこれに限られるものではない。PHS(Personal Handyphone System)などのその他の通信局に本発明を適用することも可能である。

【０１７１】また、ＩＣカード１０６がコマンドを受信すると、出力暗号化手段１１の利用者識別情報暗号化手段１２が利用者識別情報記憶手段１３に記憶された利用者識別コードを暗号化していたが、これに限られるものではない。例えば出力暗号化手段１１は、不揮発性メモリ部１０６１に利用者識別コードが記憶される際に、その利用者識別コードを暗号化してもよい。この場合、不揮発性メモリ部１０６１には、暗号化された利用者識別コードが記憶される。そして、ＩＣカード１０６がコマンドを受信する際には、出力暗号化手段１１は、予め暗号化された利用者識別コードを不揮発性メモリ部１０６１から読み出すことになる。このように、不揮発性メモリ部１０６１に予め暗号化された利用者識別コードを記憶しておくことによって、万一不揮発性メモリ部１０６１が解析されたとしても、それによって平文の利用者識別コードが採取される危険性を抑えることができる。

【０１７２】また、この例では、移動通信端末１０５の制御部１０５７が暗号化組合せ情報生成手段１５として動作したが、これに限られるものではない。例えばＩＣカード１０６の制御部１０６３を暗号化組合せ情報生成手段１５として動作させるようにしてもよい。この場合、利用者が発信を指示すると、移動通信端末１０５は、自端末識別情報記憶手段１４から自端末の端末識別コードを読み出し、読み出された端末識別コードを含むコマンドをＩＣカード１０６に送信する。ＩＣカード１０６が移動通信端末１０５からこのコマンドを受信すると、ＩＣカード１０６の暗号化組合せ情報生成手段１５は、受信されたコマンドから端末識別コードを取得する。暗号化組合せ情報生成手段１５は、この端末識別コードと出力暗号化手段１１によって生成された暗号化利用者識別コードとを用いて暗号化組合せ情報を生成する。ＩＣカード１０６は、この暗号化組合せ情報を含む応答データを移動通信端末１０５に送信する。移動通信端末１０５は、ＩＣカード１０６から応答データを受信すると、その応答データから暗号化組合せ情報を取得し、暗号化組合せ情報を含む認証要求を無線基地局に送信する。

【０１７３】このように、暗号化組合せ情報生成手段１５は、移動通信端末１０５ではなく、ＩＣカード１０６に備えても良い。

（適用例２の変形例１）適用例２では、携帯電話機１０３が認証要求を交換機１０４に送信していたが、これに限られるものではない。携帯電話機１０３を移動通信網に接続する基地局制御装置、ゲートウェイ交換機などのその他の網接続装置や、契約している利用者への課金を一括管理する課金センター装置に認証要求を送信するようにしてもよい。この場合、その網接続装置や課金センター装置に、組合せ記憶手段１７、組合せ情報復元手段１８、証明情報生成手段１９が備えられることになる。例えば課金センター装置にこれらの手段が備えられる場合、交換機１０４などの網接続装置は、携帯電話機１０３と課金センター装置との間の通信を中継することになる。

【０１７４】この中継を交換機１０４が行う場合の携帯電話機１０３、交換機１０４、課金センター装置の動作を図１７及び図１８を用いて説明する。ここで、図１７は携帯電話機１０３と交換機１０４の動作の関係を表すフローチャートであり、図１８は課金センター装置の動作を表すフローチャートである。

【０１７５】図１７に示す通り、携帯電話機１０３の動作は、図１６を用いて説明した携帯電話機のものと同様であり、図１８に示す通り、課金センター装置の動作は、認証要求が交換機１０４から転送される点と判定結果を交換機１０４に送信する点を除いて、図１６を用いて説明した交換機のものと同様である。

【０１７６】図１７に示すように、手順Ｓ１６０１乃至Ｓ１６０３に従い、暗号化組合せ情報を含む認証要求が携帯電話機１０３から交換機１０４に送信され、交換機１０４が認証要求を受信すると（Ｓ１６０４）、交換機１０４は、その認証要求を課金センター装置に転送する（Ｓ１７０１）。

【０１７７】図１８に示すように、交換機１０４から転送された認証要求を課金センター装置が受信すると（Ｓ１８０１）、課金センター装置の組合せ情報復元手段１８は、認証要求から暗号化組合せ情報を取得し、暗号化組合せ情報の暗号化利用者識別コードを復号化することによって、組合せ情報を復元する（Ｓ１８０２）。

【０１７８】組合せ情報が復元されると、証明情報生成手段１９は、復元された組合せ情報が表す利用者識別コードと端末識別コードとの組合せと一致する組合せが組合せ記憶手段１７に記憶されているか否かを判定する（Ｓ１８０３）。

【０１７９】一致する組合せがあると判定された場合、証明情報生成手段１９は、組合せ情報が正当な組合せを表すことを証明する応答データを作成する（Ｓ１８０４）。

【０１８０】これに対し、一致する組合せがないと判定された場合、証明情報生成手段１９は、組合せ情報が正当な組合せを表さないことを示す応答データを作成する（Ｓ１８０５）。

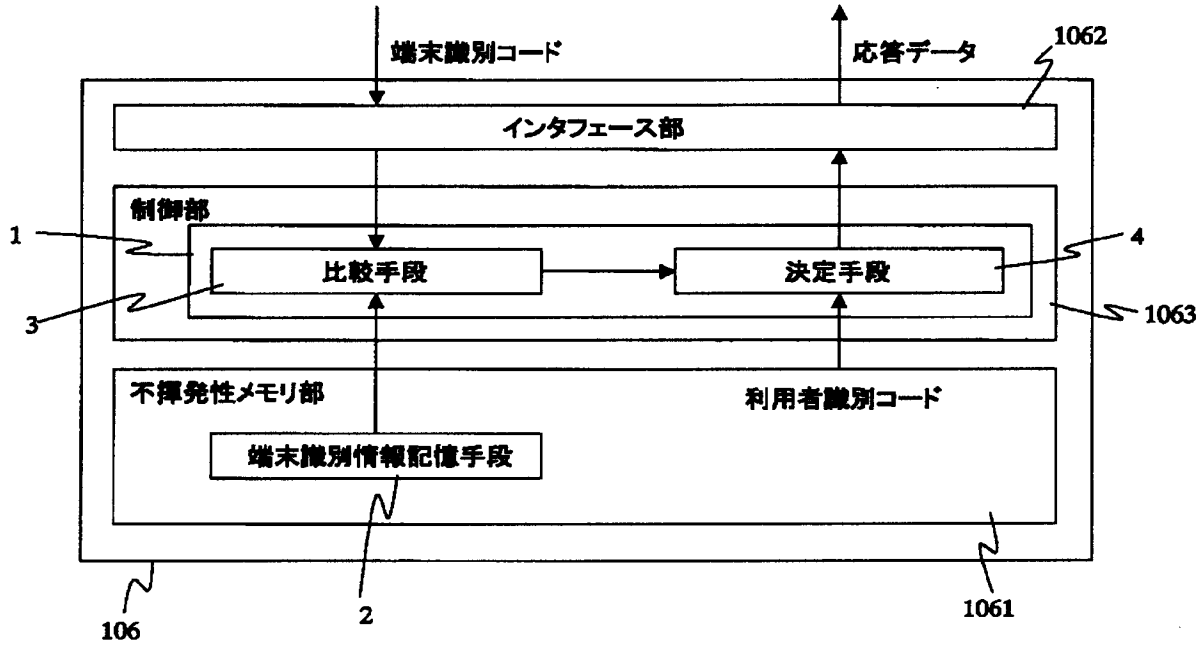
【０１８１】手順Ｓ１８０４又はＳ１８０５において作成された判定結果を表す応答データは、課金センター装

置から交換機１０４に送信される（Ｓ１８０６）。
【０１８２】交換機１０４が課金センター装置からの応答データを受信すると（Ｓ１７０２）、交換機１０４は、その応答データを携帯電話機１０３に転送する（Ｓ１６０９）。
【０１８３】携帯電話機１０３が応答データを受信すると（Ｓ１６１０）、手順Ｓ１６１１乃至Ｓ１６１３に従い、通信を許可するか禁止するかが決定される。
【０１８４】このように課金センター装置において判定を行うことによって、課金センター装置の組合せ記憶手段１７に、契約している利用者に関する情報を集約することができる。組合せ情報は、課金センター装置で復元されるから、利用者識別コードの不正利用や漏洩を防止することができる。
（適用例２の変形例２）適用例２では、利用者識別コードは、携帯電話機１０３が移動体通信網を用いて通信するのに伴って発生する課金の対象を特定するために用いられたが、これに限られるものではない。例えば電子商取引の決済に利用者識別コードが用いられることもある。この場合に、携帯電話機１０３が利用者識別コードを利用して行う電子商取引の通信を制御するようにしてもよい。
【０１８５】携帯電話機１０３が電子商取引に利用される場合、例えば図１９に示すように、携帯電話機１０３は、インターネット１０８上の電子商取引サーバ１０９に接続される。携帯電話機１０３からの通信パケットは、無線基地局装置１０１、基地局制御装置１０２、交換機１０４、基幹網１１０を通じて、ゲートウェイ交換機ゲートウェイ交換機１１１に転送される。ゲートウェイ交換機１１１は、プロトコル変換などを行うゲートウェイ装置１１２を用いて、基幹網１１０をインターネット１０８などの他の通信網と接続している。携帯端末１０３からの通信パケットは、ゲートウェイ交換機１１１、ゲートウェイ装置１１２、インターネット１０８を介して電子商取引サーバ１０９に転送される。また、電子商取引サーバ１０９からの通信パケットは、逆の経路を辿って携帯電話機１０３に転送される。電子商取引は、携帯電話機１０３が電子商取引サーバ１０９との間で取引内容を表す通信パケットを授受することによって行われる。
【０１８６】電子商取引サーバ１０９には、上述の組合せ記憶手段１７、組合せ情報復元手段１８、証明情報生成手段１９が備えられる。
【０１８７】携帯電話機１０３の通信許可決定手段１６は、組合せ情報が表す組合せは電子商取引上正当であると証明する応答データを電子商取引サーバ１０９から受信した場合にのみ、利用者識別コードによって利用者を特定する電子商取引の通信を行うことを許可する。
【０１８８】この場合の携帯電話機１０３と電子商取引サーバ１０９の動作手順は、図１６における交換機１０４を電子商取引サーバ１０９に置き換えた手順となる。
【０１８９】なお、電子商取引サーバ１０９の証明情報生成手段１９は、利用者識別コードに対応付けられた決済用口座の残高が不足しているなどの場合、利用者識別コードと端末識別コードとの組合せが正当であっても、電子商取引上正当でないとして、正当でないことを表す判定を行うようにしてもよい。
【０１９０】上述の各例におけるＩＣカードは、例えばUIMに相当するものであるが、SD(Secure Digital)メモリカードなどのメモリカードが拡張されたＩＣカードに対して本発明を適用してもよい。この場合、メモリカードのソフトウェアとハードウェアの構成は、UIMなどと同等の構成に拡張される。このような拡張されたメモリカードでは、OS(Operating System)や各種のアプリケーションが利用するライブラリも用意される。
【０１９１】
【発明の効果】以上説明した通り、本発明では、ＩＣカードが装着された携帯電話機などの端末を識別するため端末識別情報がＩＣカードに記憶された端末識別情報とは相違している場合、端末がＩＣカードに要求する利用者識別コードなどの要求情報が端末に出力されない。このため、紛失や盗難によって利用者のＩＣカードが悪意ある第三者の手に渡ったとしても、ＩＣカードの要求情報が不正利用されたり漏洩したりする恐れを抑制することができる。
【図面の簡単な説明】
【図１】　本発明の適用例１におけるＩＣカードの概略構成を示す図
【図２】　本発明が適用される携帯電話機を含む移動通信システムの構成を簡略的に示す図
【図３】　携帯電話機のハードウェア構成を説明するための図
【図４】　本発明の適用例１におけるＩＣカードによる通信制御方法を説明するためのフローチャート
【図５】　本発明の適用例１における他のＩＣカードの概略構成を示す図
【図６】　本発明の適用例１における移動通信端末の概略構成を示す図
【図７】　本発明の適用例１におけるＩＣカードと移動通信端末の動作の関係を説明するためのフローチャート
【図８】　本発明の適用例１の変形例１におけるＩＣカードの概略構成を示す図
【図９】　適用例１の変形例１におけるＩＣカードと移動通信端末の動作の関係を説明するためのフローチャート
【図１０】　適用例１の変形例１における他のＩＣカードの概略構成を示す図
【図１１】　本発明の適用例１の変形例２における携帯電話機の概略構成を示す図
【図１２】　適用例１の変形例２におけるパスワードを

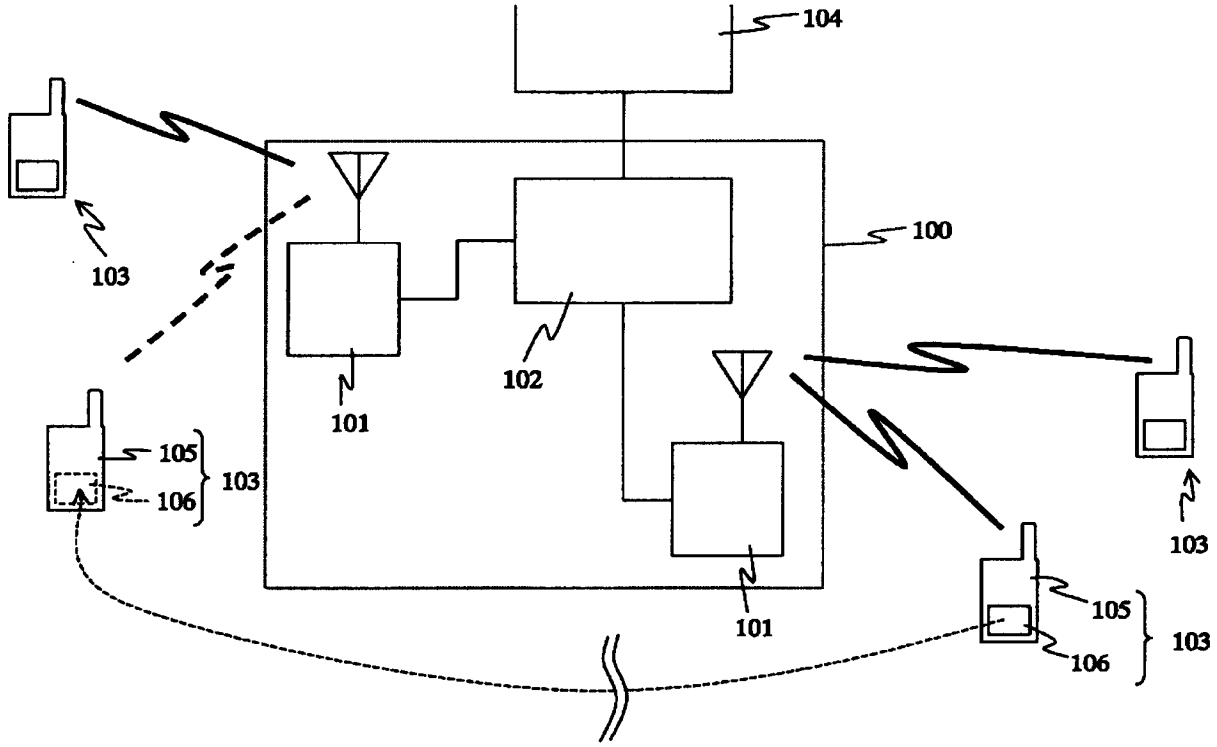
変更する手順を示すフローチャート
【図１３】　本発明の適用例２における携帯電話機の概略構成を示す図
【図１４】　本発明の適用例２における交換機の概略構成を示す図
【図１５】　本発明の適用例２における組合せ記憶手段の記憶内容を示す図
【図１６】　本発明の適用例２における携帯電話機による通信制御方法を説明するためのフローチャート
【図１７】　本発明の適用例２の変形例１における携帯電話機と課金センター装置との通信手順を説明するためのフローチャート
【図１８】　本発明の適用例２の変形例１における携帯電話機と課金センター装置との通信手順を説明するための他のフローチャート
【図１９】　携帯電話機と電子商取引サーバとの接続関係を説明するための図
【符号の説明】

1	許可決定手段
2	端末識別情報記憶手段
3	比較手段
4	決定手段
5	暗号化手段
6	通信許可決定手段
7	自端末識別情報記憶手段
8	認証情報記憶手段
9	端末識別情報更新手段
１０	認証情報変更手段
１１	出力暗号化手段
１２	利用者識別情報暗号化手段
１３	利用者識別情報記憶手段
１４	自端末識別情報記憶手段
１５	暗号化組合せ情報生成手段
１６	通信許可決定手段
１７	組合せ記憶手段
１８	組合せ情報復元手段
１９	証明情報生成手段
１０３	携帯電話機
１０４	交換機
１０５	移動通信端末
１０６	ＩＣカード
１０９	電子商取引サーバ

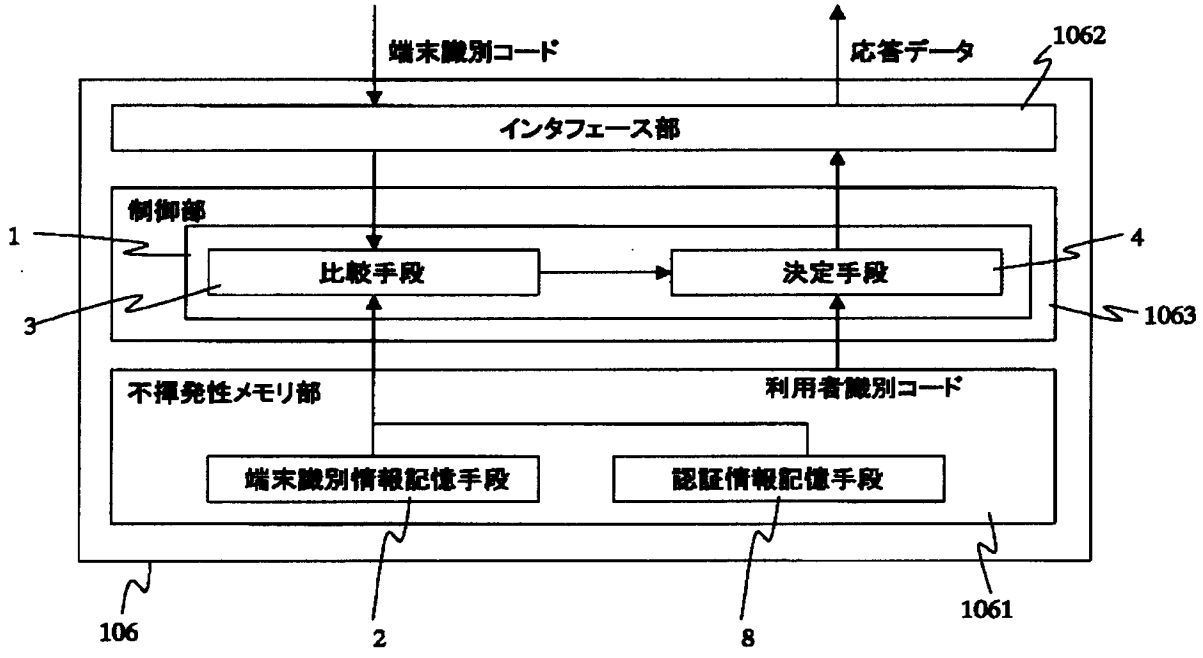
【図１】



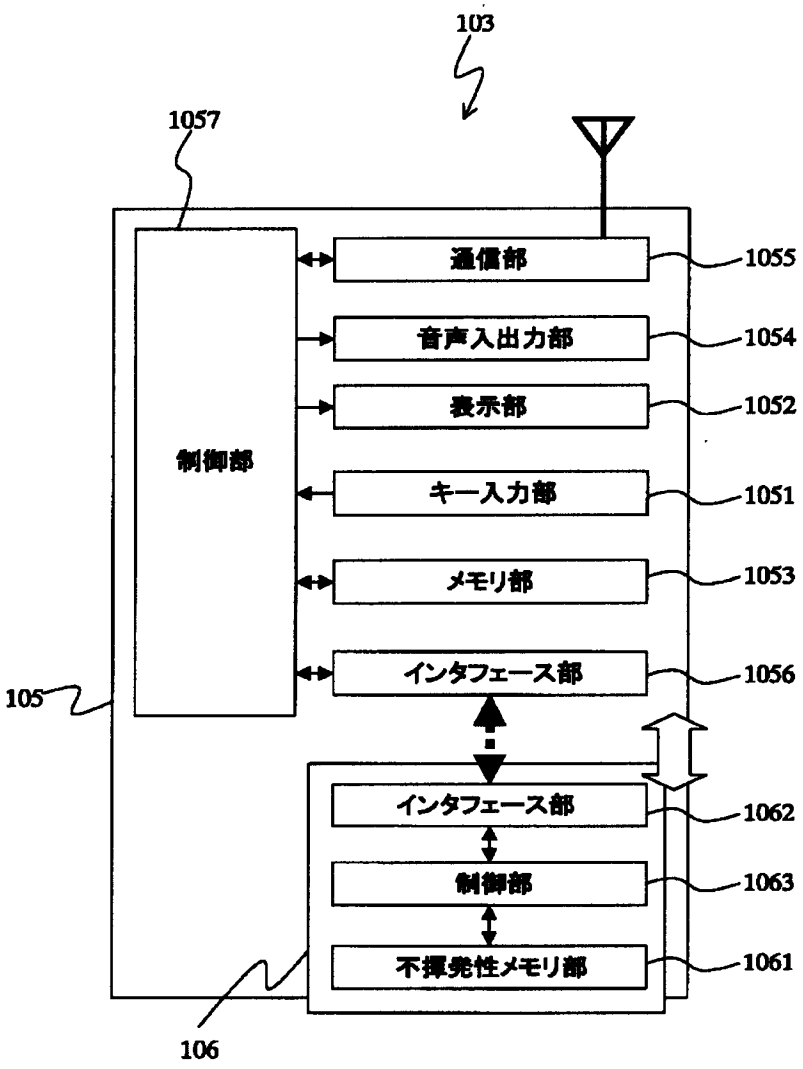
【図２】


104
100
103
101
102
105
106
103
101
105
106
103
103

【図８】


端末識別コード
応答データ
1062
インタフェース部
制御部
1
比較手段
決定手段
4
3
1063
不揮発性メモリ部
利用者識別コード
端末識別情報記憶手段
認証情報記憶手段
106
2
8
1061

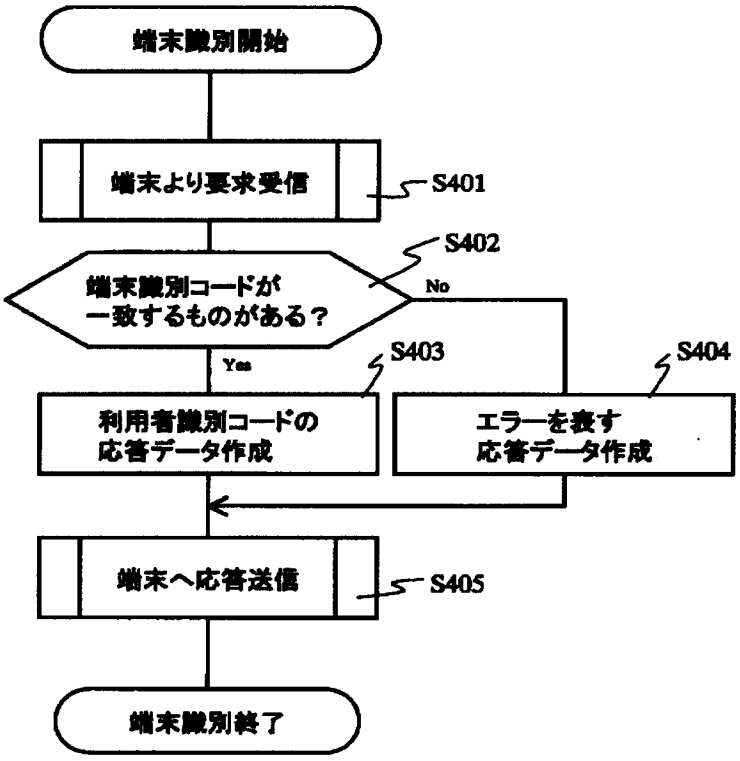
【図３】



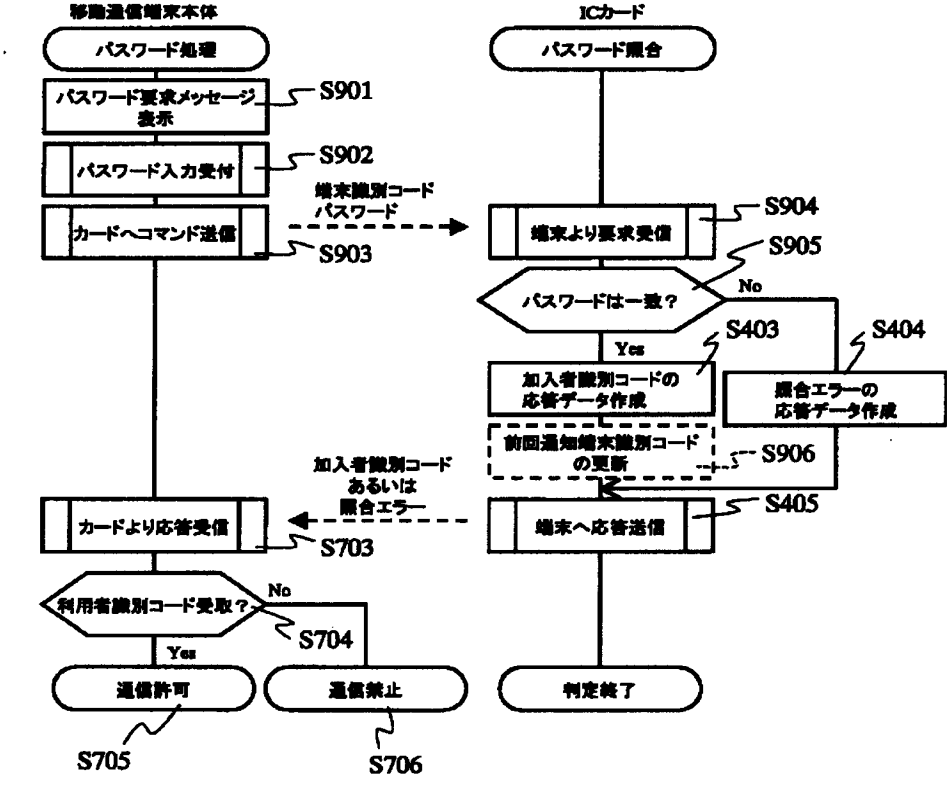
【図１５】

利用者識別コード	端末識別コード
利用者識別コード	端末識別コード
利用者識別コード	端末識別コード
:	:
利用者識別コード	端末識別コード

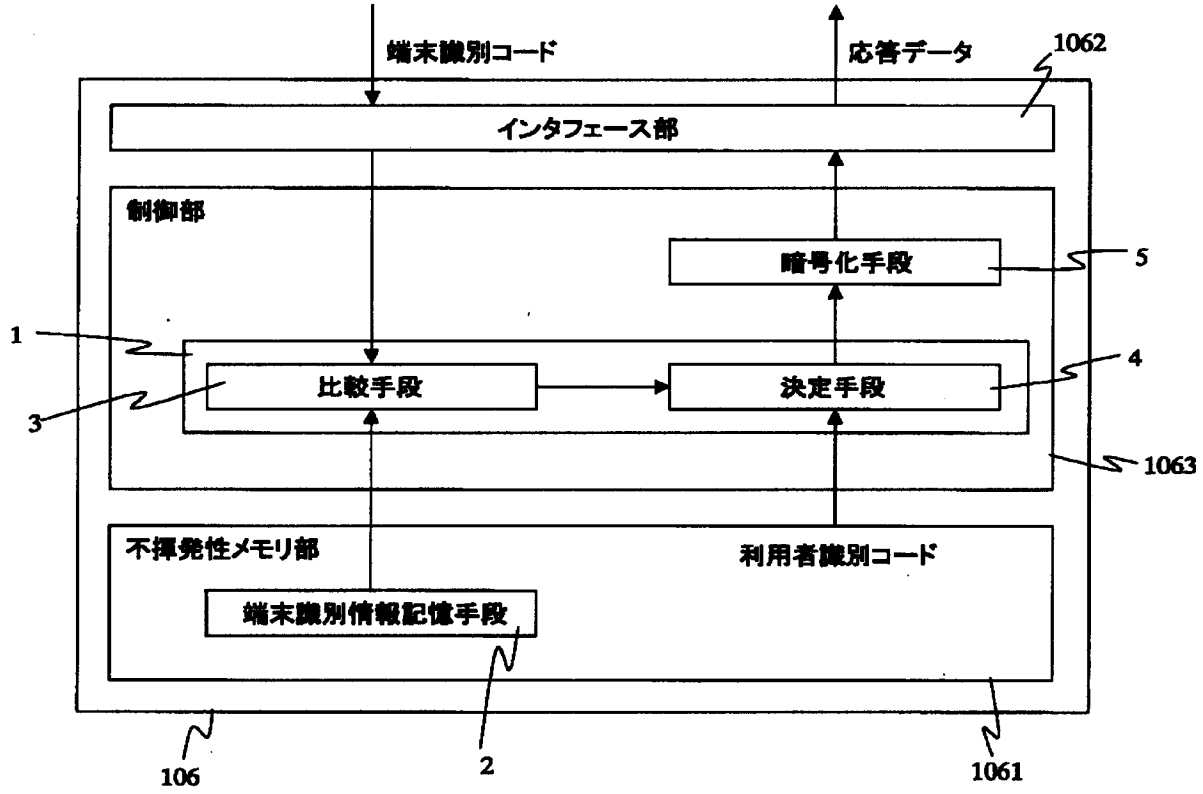
【図４】


端末識別開始
端末より要求受信
S401
S402
端末識別コードが
一致するものがある？
No
Yes
S403
S404
利用者識別コードの
応答データ作成
エラーを表す
応答データ作成
端末へ応答送信
S405
端末識別終了

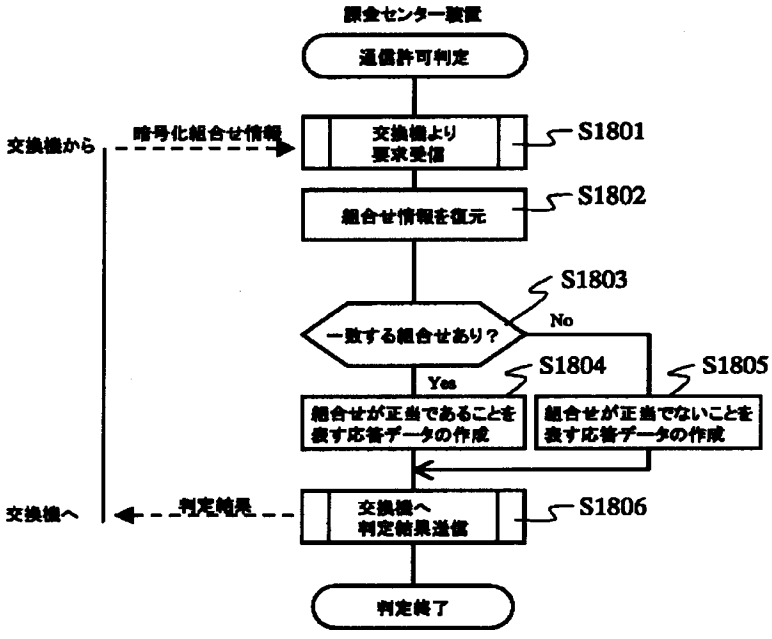
【図９】


移動通信端末本体
ICカード
パスワード処理
パスワード照合
パスワード要求メッセージ
表示
S901
パスワード入力受付
S902
端末識別コード
パスワード
カードへコマンド送信
S903
端末より要求受信
S904
S905
パスワードは一致？
No
Yes
S403
S404
加入者識別コードの
応答データ作成
照合エラーの
応答データ作成
前回通知端末識別コード
の更新
S906
加入者識別コード
あるいは
照合エラー
カードより応答受信
S703
端末へ応答送信
S405
利用者識別コード受取？
No
S704
Yes
通信許可
通信禁止
判定終了
S705
S706

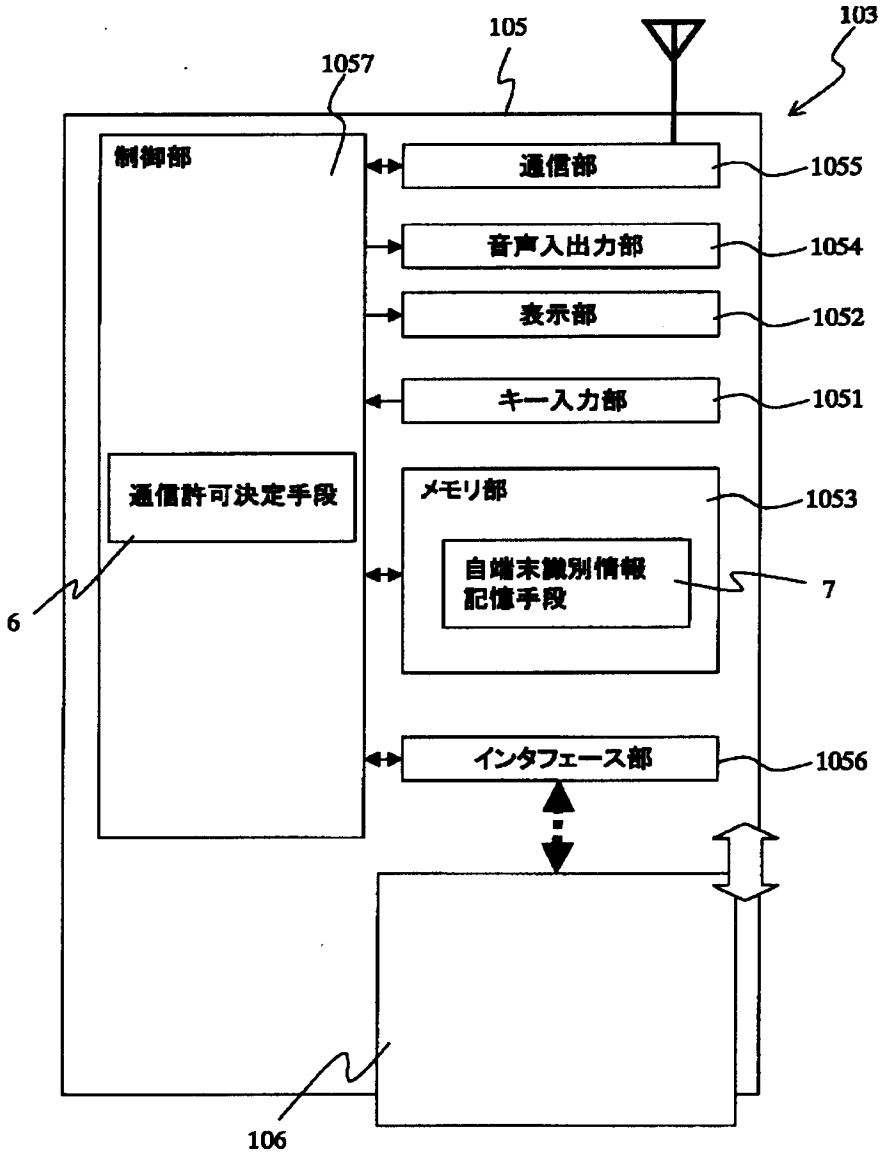
【図５】


端末識別コード
応答データ
1062
インタフェース部
制御部
暗号化手段
5
1
比較手段
決定手段
4
3
1063
不揮発性メモリ部
利用者識別コード
端末識別情報記憶手段
106
2
1061

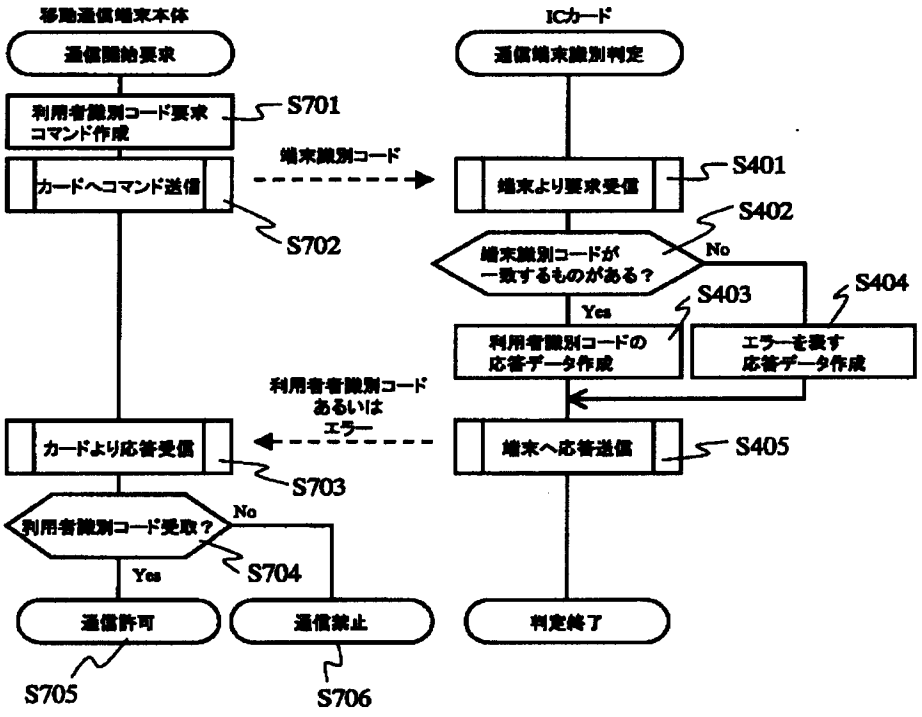
【図１８】


課金センター装置
通信許可判定
交換機から
暗号化組合せ情報
交換機より
要求受信
S1801
組合せ情報を復元
S1802
S1803
一致する組合せあり？
No
Yes
S1804
S1805
組合せが正当であることを
表す応答データの作成
組合せが正当でないことを
表す応答データの作成
交換機へ
判定結果
交換機へ
判定結果送信
S1806
判定終了

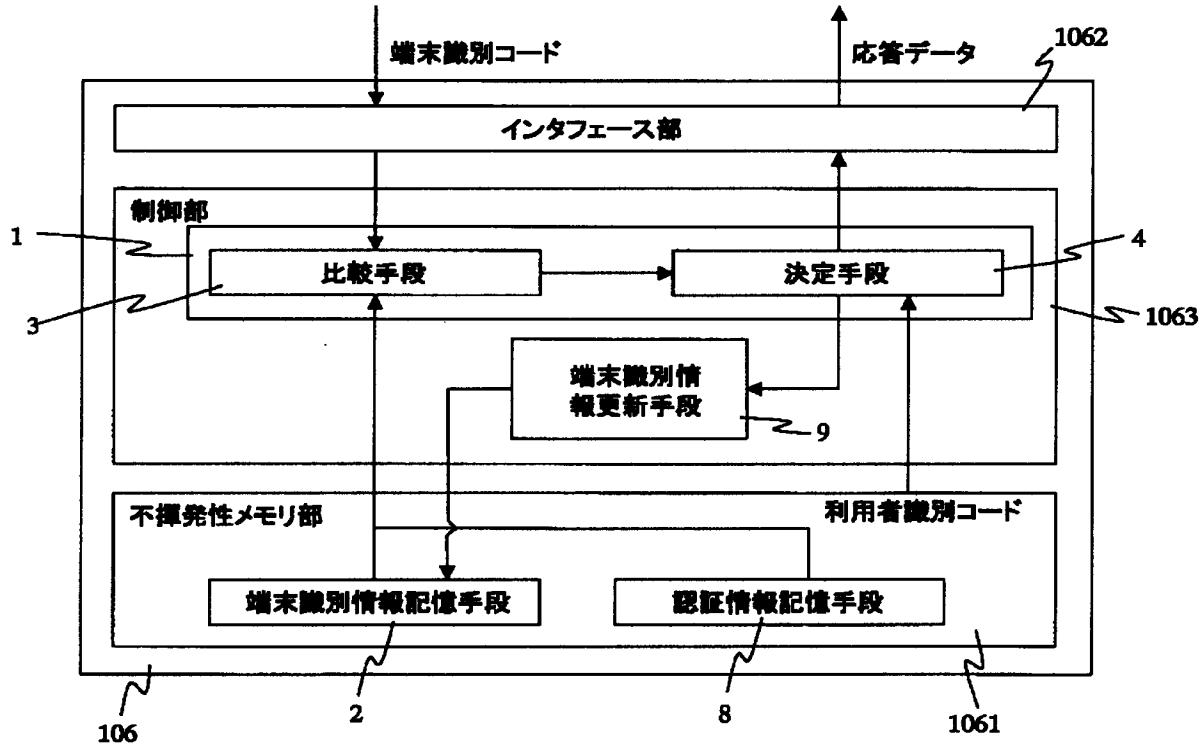
【図６】


103
105
1057
制御部
通信部
1055
音声入出力部
1054
表示部
1052
キー入力部
1051
通信許可決定手段
メモリ部
1053
自端末識別情報
記憶手段
7
6
インタフェース部
1056
106

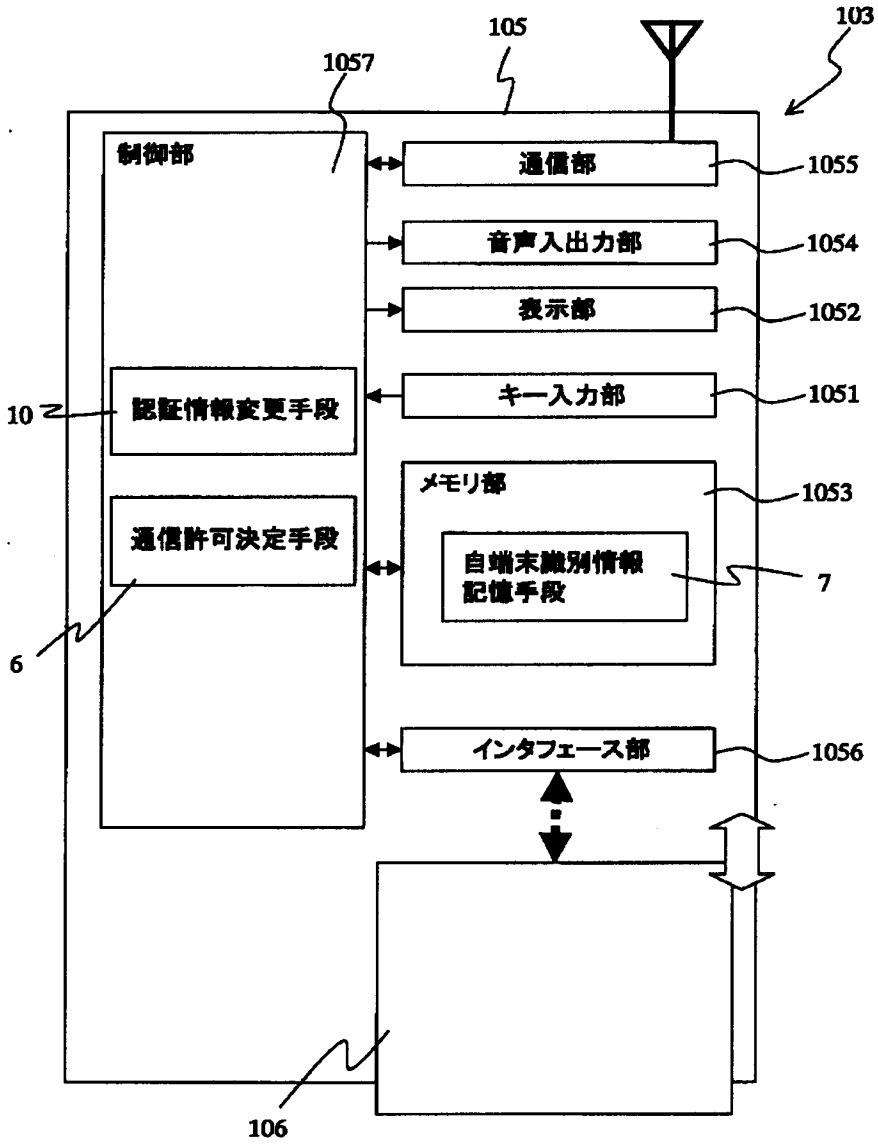
【図７】


移動通信端末本体
ICカード
通信開始要求
通信端末識別判定
利用者識別コード要求
コマンド作成
S701
端末識別コード
カードへコマンド送信
端末より要求受信
S401
S702
S402
端末識別コードが
一致するものがある？
No
S404
S403
Yes
利用者識別コードの
応答データ作成
エラーを表す
応答データ作成
利用者識別コード
あるいは
エラー
カードより応答受信
端末へ応答送信
S405
S703
利用者識別コード受取？
No
S704
Yes
通信許可
通信禁止
判定終了
S705
S706

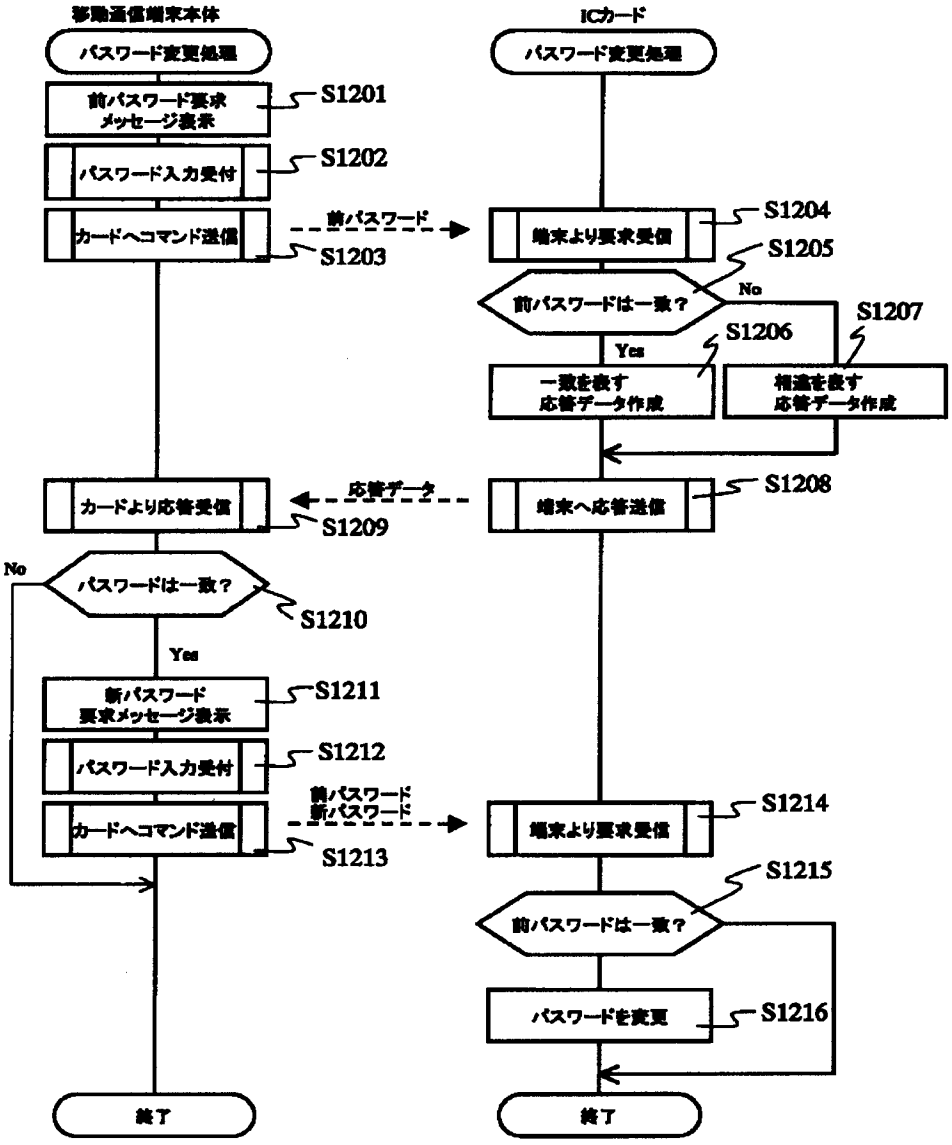
【図１０】


端末識別コード
応答データ
1062
インタフェース部
制御部
1
比較手段
決定手段
4
3
1063
端末識別情
報更新手段
9
不揮発性メモリ部
利用者識別コード
端末識別情報記憶手段
認証情報記憶手段
106
2
8
1061

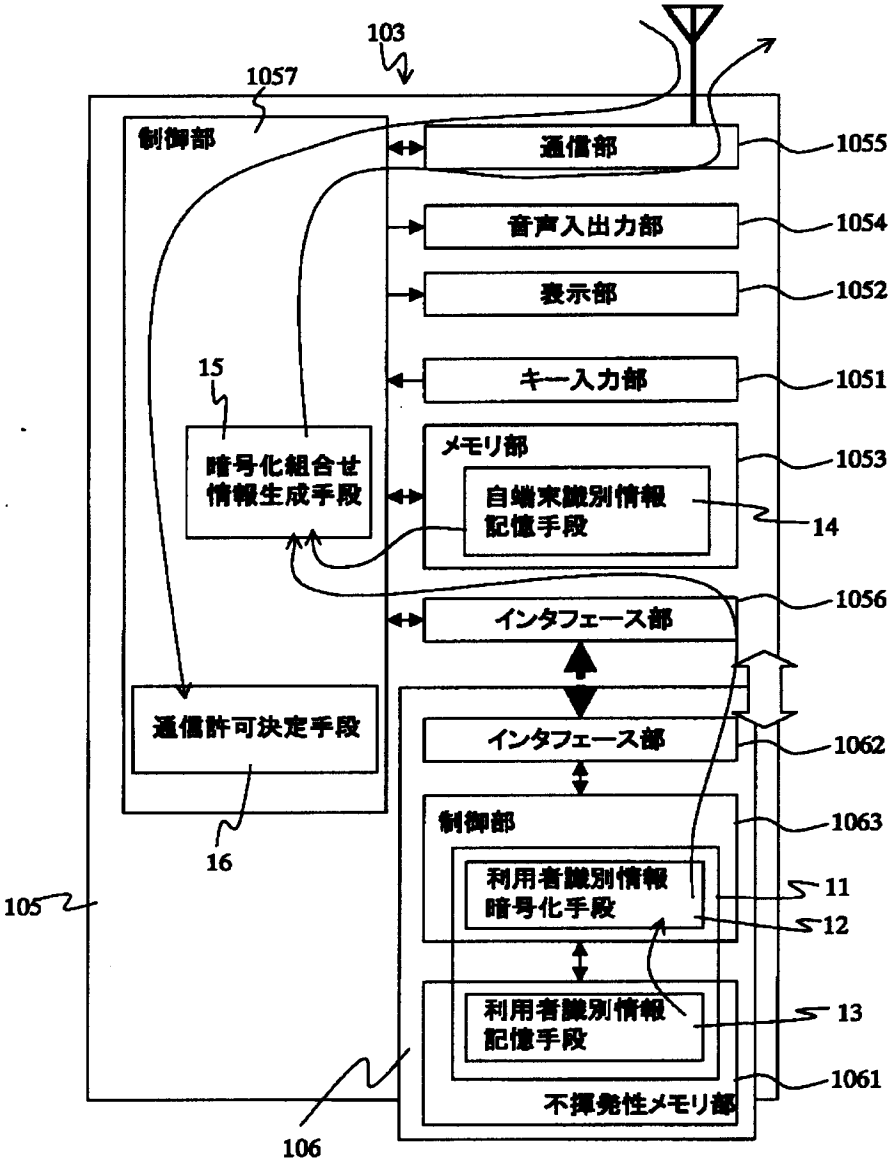
【図１１】


103
105
1057
制御部
通信部
1055
音声入出力部
1054
表示部
1052
キー入力部
1051
10
認証情報変更手段
メモリ部
1053
通信許可決定手段
自端末識別情報
記憶手段
7
6
インタフェース部
1056
106

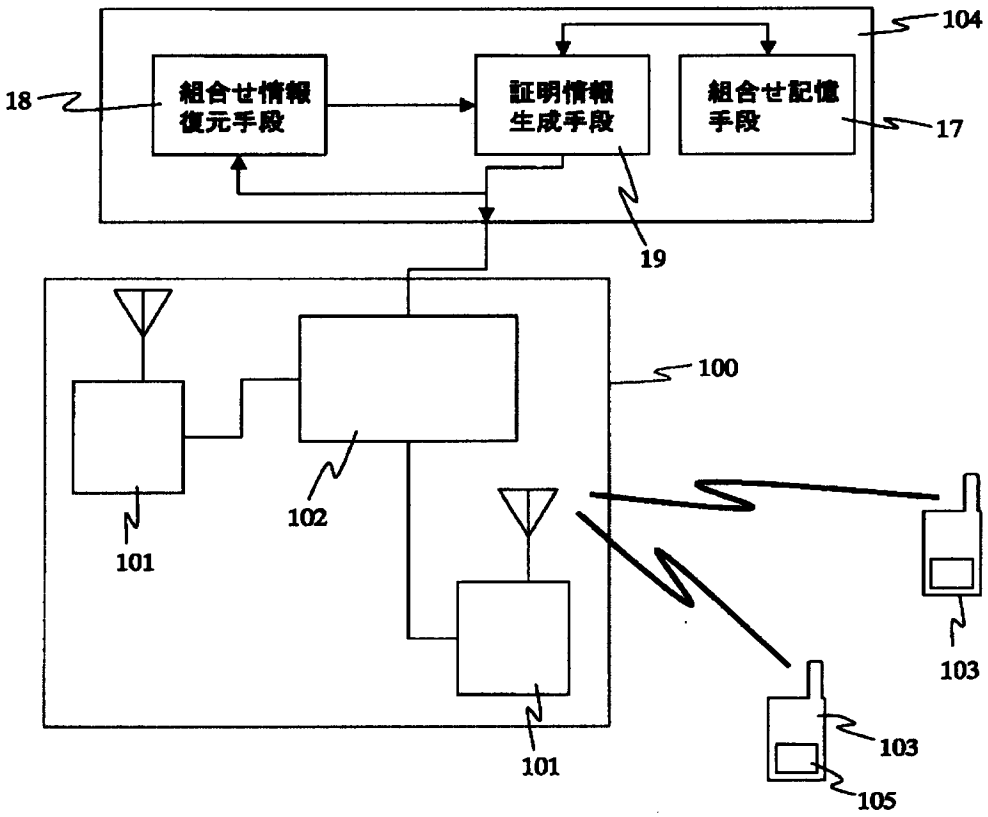
【図１２】


移動通信端末本体
ICカード
パスワード変更処理
パスワード変更処理
前パスワード要求
メッセージ表示
S1201
パスワード入力受付
S1202
カードへコマンド送信
前パスワード
S1203
端末より要求受信
S1204
S1205
前パスワードは一致？
No
S1207
Yes
S1206
一致を表す
応答データ作成
相違を表す
応答データ作成
カードより応答受信
応答データ
S1209
端末へ応答送信
S1208
No
パスワードは一致？
S1210
Yes
新パスワード
要求メッセージ表示
S1211
パスワード入力受付
S1212
カードへコマンド送信
前パスワード
新パスワード
S1213
端末より要求受信
S1214
S1215
前パスワードは一致？
パスワードを変更
S1216
終了
終了

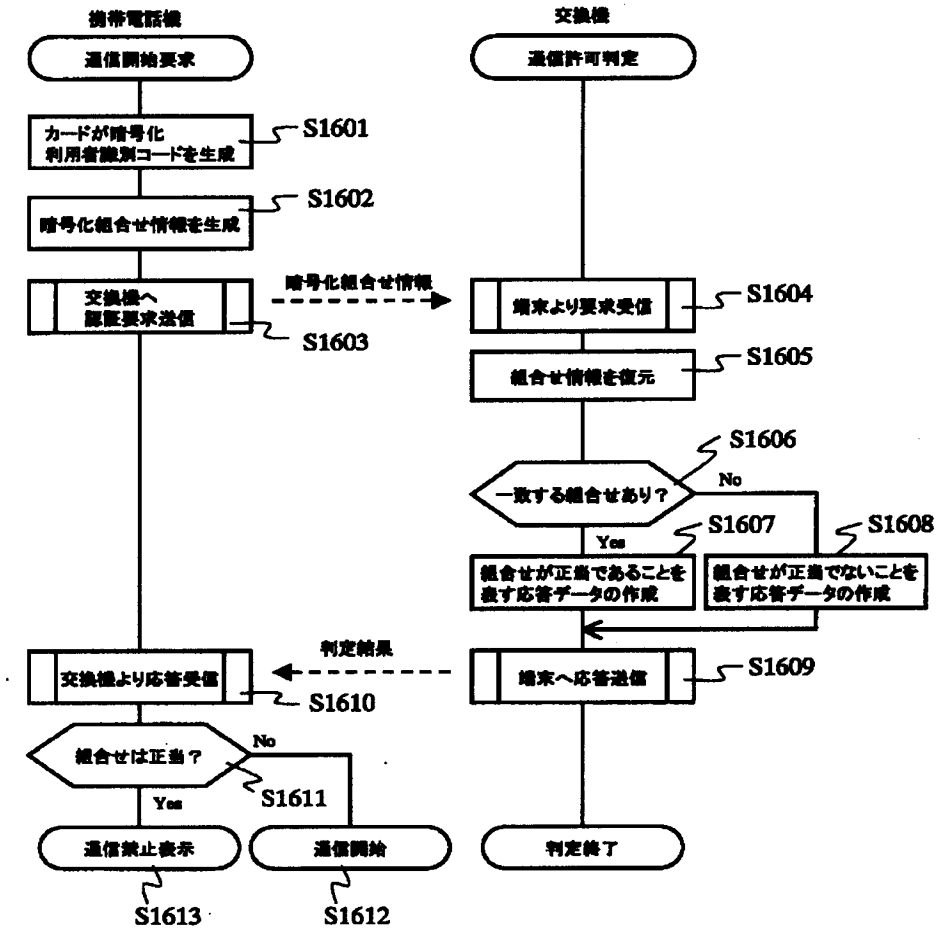
【図１３】


103
1057
制御部
通信部
1055
音声入出力部
1054
表示部
1052
15
キー入力部
1051
暗号化組合せ情報生成手段
メモリ部
1053
自端末識別情報記憶手段
14
1056
インタフェース部
通信許可決定手段
インタフェース部
1062
制御部
1063
利用者識別情報暗号化手段
11
12
利用者識別情報記憶手段
13
1061
不揮発性メモリ部
16
105
106

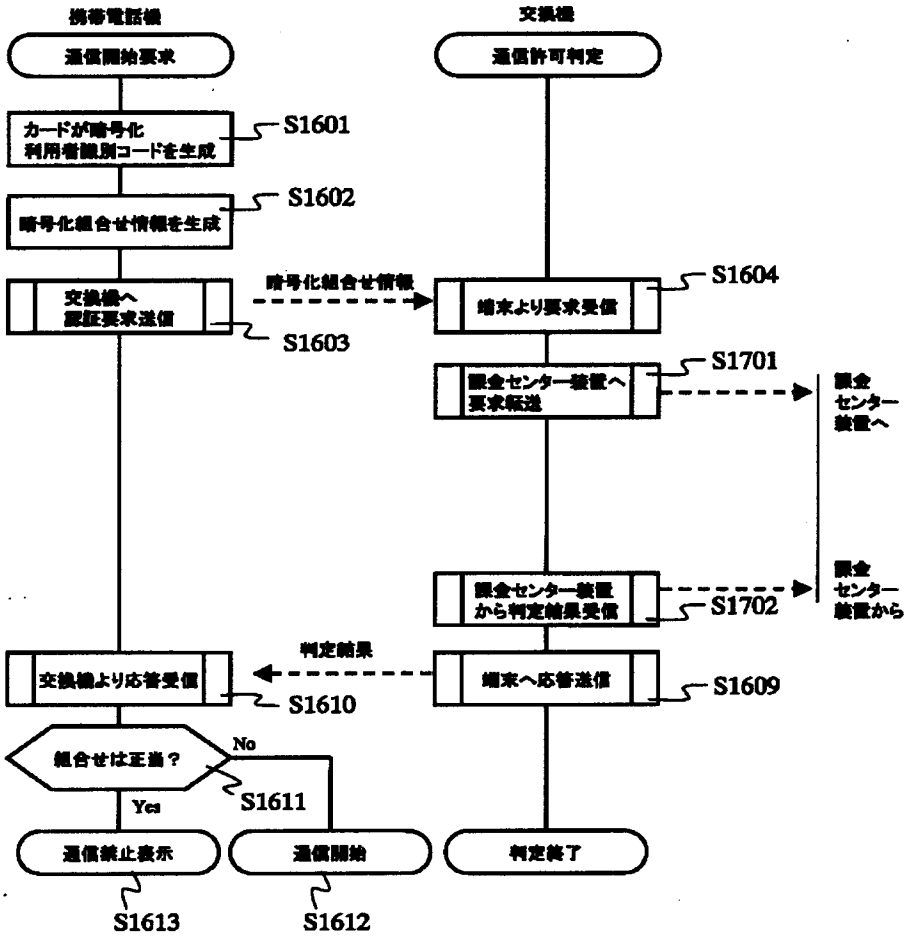
【図１４】


104
18
組合せ情報
復元手段
証明情報
生成手段
組合せ記憶
手段
17
19
100
101
102
101
103
103
105

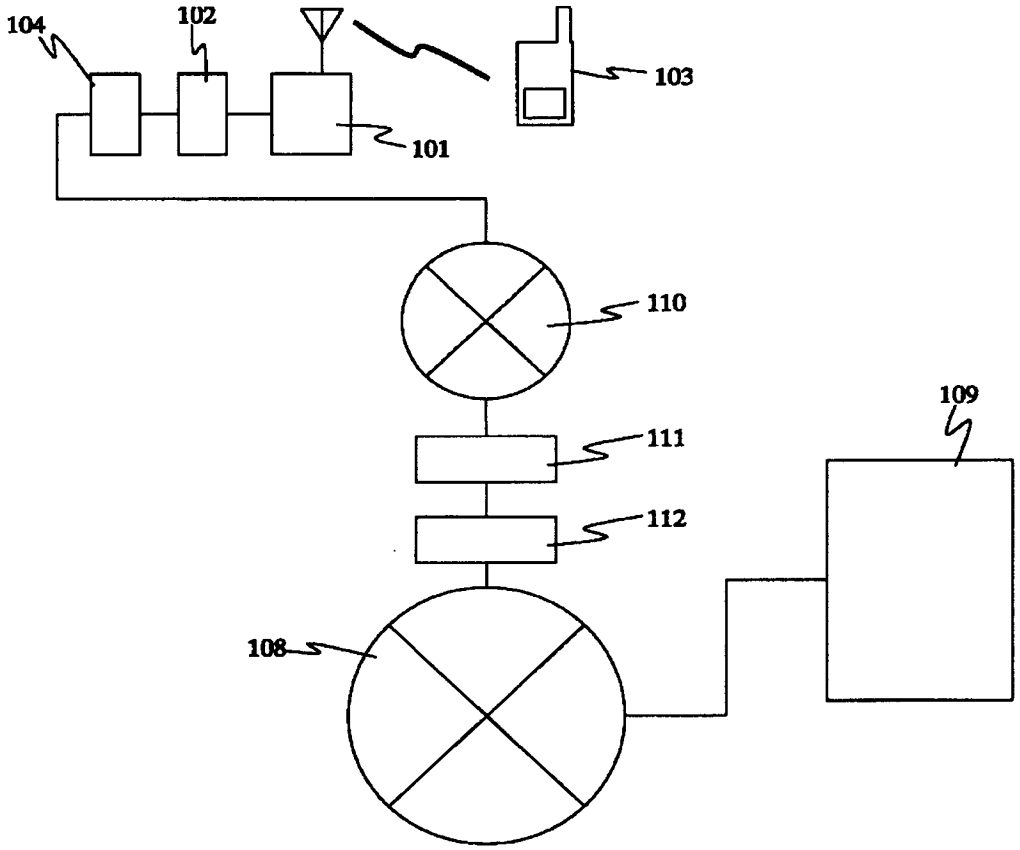
【図１６】


携帯電話機
交換機
通信開始要求
通信許可判定
カードが暗号化
利用者識別コードを生成
S1601
暗号化組合せ情報を生成
S1602
交換機へ
認証要求送信
S1603
暗号化組合せ情報
端末より要求受信
S1604
組合せ情報を復元
S1605
S1606
一致する組合せあり？
No
Yes
S1607
S1608
組合せが正当であることを
表す応答データの作成
組合せが正当でないことを
表す応答データの作成
判定結果
交換機より応答受信
S1610
端末へ応答送信
S1609
組合せは正当？
No
S1611
Yes
通信禁止表示
通信開始
判定終了
S1613
S1612

【図１７】


携帯電話機
交換機
通信開始要求
通信許可判定
カードが暗号化
利用者識別コードを生成
S1601
暗号化組合せ情報を生成
S1602
交換機へ
認証要求送信
暗号化組合せ情報
S1603
端末より要求受信
S1604
課金センター装置へ
要求転送
S1701
課金
センター
装置へ
課金センター装置
から判定結果受信
S1702
課金
センター
装置から
判定結果
交換機より応答受信
S1610
端末へ応答送信
S1609
組合せは正当？
No
S1611
Yes
通信禁止表示
通信開始
判定終了
S1613
S1612

【図１９】



フロントページの続き

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ（参考）
Ｈ０４Ｍ 3/42		Ｇ０６Ｋ 19/00	Ｐ ５Ｋ０６７

Ｆターム(参考) 5B017 AA06 BB09 BB10 CA14
5B035 AA13 BB09 CA11
5B058 CA27 KA31 KA35 YA20
5K024 AA63 BB04 CC11
5K027 AA11 BB09
5K067 AA32 BB04 DD17 EE02 EE16
HH32 HH36 KK13 KK15